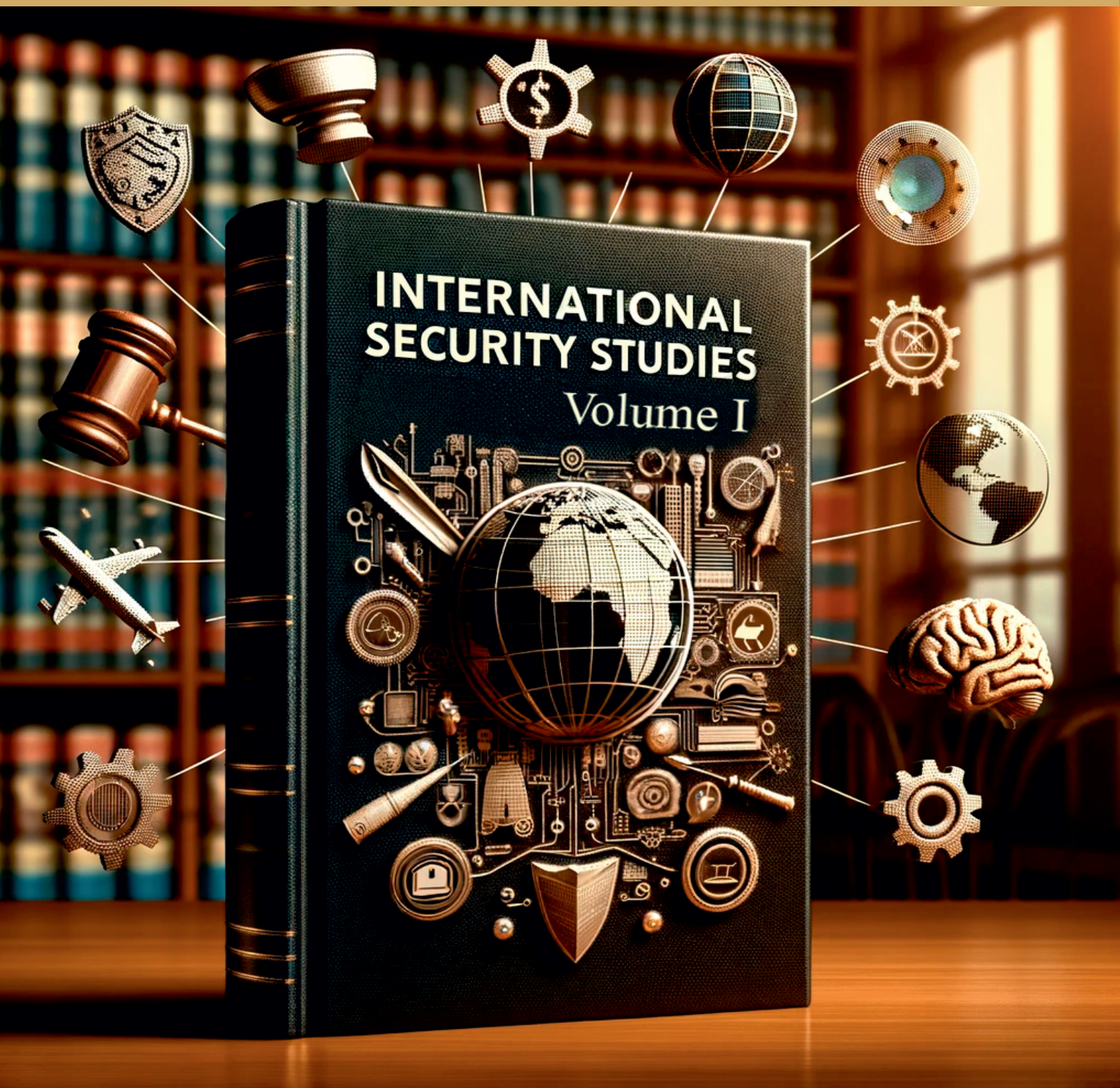
INTERNATIONAL SECURITY STUDIOS: MANAGERIAL, TECHNICAL, LEGAL, ENVIRONMENTAL, INFORMATIVE AND PSYCHOLOGICAL ASPECTS



Norwegian University of Life Sciences

INTERNATIONAL SECURITY STUDIOS: managerial, technical, legal, environmental, informative and psychological aspects

international collective monograph

Volume I

Oslo, Kingdom of Norway – 2024

UDC 327(100)-049.5
I 61
DOI 10.5281/zenodo.10828981

Recommended for publication by the academic council of NMBU (protocol №. 12 dated 11. 03.2024)

M 58 International security studios: managerial, technical, legal, environmental, informative and psychological aspects. *International collective monograph. Volume I. NMBU, Research and Education*. 2024. – 700 p.

The International collective monograph is the result of the generalization of the conceptual work of scientists who consider current topics from such fields of knowledge as: management, technical sciences, law, ecology, information sciences and psychological sciences through the prism of international security studies.

For scientists, educational staff, PhD candidates, masters of educational institutions, university faculties, stakeholders, managers and employees of management bodies at various hierarchical levels, and for everyone, who is interested in current problems of management, technical sciences, law, ecology, information sciences and psychological sciences through the prism of international security studies.

ISBN 978-82-327-0549-9

AUTHORS:

CHAPTER 1.
Andrej LIPTÁK
Senior officer specialist Financial Investigation Department,
National Centre for Specific Crimes
Ministry of Interior of the Slovak republic
(Pribinova 2, 812 72 Bratislava,
Slovak republic)
andrej.liptak@minv.sk
https://www.researchgate.net/profile/Andrej-Liptak/research

CHAPTER 2.
Nadiya BAKALO
PhD (Economics), Associate Professor,
Associate professor international economic relations and tourism department
National University «Yuri Kondratyuk Poltava Polytechnic»
(Poltava, Pershotravnevaya avenue, 24, Ukraine)
bakalo.nv@ukr.net
https://orcid.org/0000-0002-3260-412X

Viktoriia MAKHOVKA
PhD (Economics)
National University «Yuri Kondratyuk Poltava Polytechnic»
(Poltava, Pershotravnevaya avenue, 24, Ukraine)
mahovkavm@gmail.com
https://orcid.org/0000-0001-7985-7792

CHAPTER 3.
Nataliia BORYSENKO,
Doctor of Philosophy (Pedagogy), Associate Professor, Vice-rector for Educational Work,
H. S. Skovoroda Kharkiv National Pedagogical University (Kharkiv, Ukraine)
bna0301@gmail.com
https://orcid.org/0000-0002-0532-3867

Olena GRECHANYK,
Candidate of Pedagogical Sciences, Associate Professor,
Head of the Department of Scientific Foundations of Management,
H. S. Skovoroda Kharkiv National Pedagogical University (Kharkiv, Ukraine)
grechaniklena@ukr.net
https://orcid.org/0000-0002-4671-0724

CHAPTER 4.
Olha DZHYHORA,
PhD in Economics, Associate Professor,
Associate Professor of the Department of National Security, Public Management and Administration, Zhytomyr Polytechnic State University,
(103 Chudnivska St., Zhytomyr, Ukraine),
kebpua_dom@ztu.edu.ua,
https://orcid.org/0000-0001-8490-3917

AUTHORS:

CHAPTER 5.

Maryna HALKEVYCH
Ph.D. in Economics, Associate Professor of Department of Business and Tourism Management, Izmail University of Humanities (12, Repin street, Izmail, Odesa region, 68600, Ukraine)
halkevych_maryna@ukr.net
https://orcid.org/0000-0002-4786-4856

CHAPTER 6.

Andrii HOLOVNIA
Doctor of Philosophy, Senior Lecturer at the Department of Professional Training of the Retraining and Advanced Training Centre of the National Academy of the National Guard of Ukraine
golovnijandr1@ukr.net
https://orcid.org/0000-0001-9188-0055

Volodymyr TROBIUK
Candidate of Military Sciences, Associate Professor, Head of the Educational and Research Centre for the Organization of the Educational Process of the National Academy of the National Guard of Ukraine,
D1ss@ukr.net
https://orcid.org/0000-0002-3248-2935

CHAPTER 7.

Sergii V. IVANOV
Doctor of Economic Sciences, Professor, General Director of LLC «Alcohol and non-alcoholic plant «Dnepr», Associate Member of the National Academy of Sciences of Ukraine
(St. Sviatoslav Khrabroho, 12 Dnipro, 49000, Ukraine)
ivanovsv@abkdnipro.com
https://orcid.org/0000-0002-1205-3797

Hanna V. RAZUMOVA
Doctor of Economic Sciences, Associate Professor,
Professor of the Department of Marketing and Business Administration,
SHEI «Priazovsky State Technical University»
(St. Gogolya, 29, Dnipro, 49000, Ukraine)
anna.raz888@gmail.com
https://orcid.org/0000-0003-4432-4050

CHAPTER 8.

Iryna KALINA
Dr.Sc. (Econ), . Ph.D., Professor of Marketing
Educational and scientific institute of economic and business management,
Interregional Academy of Personnel Management,
Kyiv, Ukraine
2 Frometivska Street, Kyiv, Ukraine
kalinargz@gmail.com,
https://orcid.org/0000-0001-5662-6967

AUTHORS:

CHAPTER 9.

Victoria KOVALENKO
D.Sc. in Economics, Professor
Odesa National University of Economics,
Department of Banking
(8 Preobrazhenskaya Str., Odesa, 65082,
Ukraine)
kovalenko-6868@ukr.net
https://orcid.org/0000-0003-2783-186X

CHAPTER 10.

Alevtyna PAKULINA
Ph.D. economy sciences, associate professor
Department of Economics and marketing
O.M. Beketov National University of Urban
Economy in Kharkiv,
(Marshal Bazhanov Street 17, Kharkiv,
Ukraine, 61002)
alevtina.pakulina@gmail.com
http://orcid.org/0000-0002-2578-9701

CHAPTER 11.

Serhii PISAREVSKYI
PhD in public administration,
senior lecturer of the Department of Logistics
Management of the Operational Faculty,
National Academy of the National Guard of
Ukraine
(Kharkiv, 3 Zahysnykiv Ukrainy Maidan),
psv021180@ukr.net
https: //orcid.org /0000-0002-2537-0767

CHAPTER 12.

Valentyna POSTOVA
PhD in Economics, Associate Professor of the
Department
of Tourism and Hotel and Restaurant Business,
Vinnytsia Institute of Trade and Economics
of State University of Trade and Economics
(Soborna, 87, 21000, Vinnytsia, Ukraine)
v.postova@vtei.edu.ua
https://orcid.org/0000-0002-0056-5648

CHAPTER 13.

Kostyantyn SPORYSHEV
candidate of technical sciences,
assistant professor
National Academy of the National Guard of
Ukraine,
(3, Maidan Zahisnykyv Ukrainy, Kharkiv,
61001, Ukraine)
spor_kos@ukr.net
https://orcid.org/0000-0003-4737-9698

CHAPTER 14.

Vladyslav YEMANOV
Doctor of scienes in public administration,
senior research
National Academy of the National Guard of
Ukraine,
(3, Maidan Zahisnykyv Ukrainy, Kharkiv,
61001, Ukraine)
mail@nangu.edu.ua
https://orcid.org/0000-0001-5055-8852

CHAPTER 15.

Vasyl KOKHANOVSKYI
PhD in Engineering, Associate professor
Associate professor of Department of Printing
Machines and Automated Complexes
Igor Sikorsky Kyiv Polytechnic Institute
(Kyiv, Ukrainę)
v.kokhanovskyi@kpi.ua
https://orcid.org/0009-0002-4804-884X

AUTHORS:

CHAPTER 16.

Hanna KYRYCHENKO
Doctor of Technical Sciences, Professor
State University of Infrastructure and Technologies, Department of Transport Technologies and Transportation Processes Operation,
(9, Kyrylivska Street, Kyiv, 04071, Ukraine)
kyrychenko_gi@gsuite.duit.edu.ua
https://orcid.org/0000-0002-6883-1877

Yuliia BERDNYCHENKO
Candidate of Historical Sciences, Associate Professor
State University of Infrastructure and Technologies, Department of Transport Technologies and Transportation Processes Operation,
(9, Kyrylivska Street, Kyiv, 04071, Ukraine)
berdnichenko_ya@gsuite.duit.edu.ua
https://orcid.org/0000-0001-7536-7155

CHAPTER 17.

Serhii YESAULOV
Candidate of Technical Sciences,
Associate Professor,
Associate Professo of the Department of Electric Transport,
O.M.Beketov National University of Urban Economy in Kharkiv,
(17, Marshal Bazhanov Street, Kharkiv, 61002, Ukraine)
serhii.yesaulov@kname.edu.ua
https://orcid.org/0009-0006-3274-716X

Olha BABICHEVA
Candidate of Technical Sciences,
Associate Professor,
Associate Professor of the Department of Electric Transport,
O.M.Beketov National University of Urban Economy in Kharkiv,
(17, Marshal Bazhanov Street, Kharkiv, 61002, Ukraine)
olga.babicheva@kname.edu.ua
https://orcid.org/0009-0003-1294-2740

CHAPTER 18.

Valentyn DIACHENKO
Candidate of Economic Sciences,
Associate Professor of the Department of Cybersecurity, IT and Economics,
Kyiv University of Intellectual Property and Law, National University "Odesa Law Academy" (210, Kharkiv highway, Kyiv, 02121 Ukraine)

dyachenko v@ukr.net
https://orcid.org/ 0000-0002-0055-9256

Nataliia DIACHENKO
Candidate of Sciences in Public Administration,
Associate Professor of the Department of Cybersecurity, IT and Economics,
Kyiv University of Intellectual Property and Law, National University "Odesa Law Academy" (210, Kharkiv highway, Kyiv, 02121 Ukraine)

n.diachenko@ukr.net

https://orcid.org/0000-0002-4306-7665

CHAPTER 19.

Iaroslav DOROHYI
DSc., Professor, Professor of Department Applied Mathematics and Informatics,
Donetsk National Technical University,
yaroslav.dorohyi@donntu.edu.ua,
https://orcid.org/0000-0003-3848-9852

Olena DOROHA-IVANIUK
Teacher of the highest category in informatics,
Pology Lyceum of Kovalivsk Village Council,
Belotserkiv District, Kyiv Region
dioo@polohivskyinvk.net
https://orcid.org/0000-0003-3640-6312

Iryna BERDYCHENKO
PhD in Law, Associate Professor of Department of Criminal Law and Procedure,
Kyiv University of Law of the National Academy of Sciences of Ukraine,
irinaberdychenko@gmail.com,
https://orcid.org/0000-0002-6670-433X

AUTHORS:

CHAPTER 20.

Olena HAITAN
Senior Lecturer
National University «Yuri Kondratyuk Poltava Polytechnic»
Department of Computer and Information Technologies and Systems
(Poltava, Ukraine)
olena.haitan@gmail.com
https://orcid.org/0000-0002-7228-9937

CHAPTER 21.

Vladyslav NEBESNIUK
Software Engineer,
Zaporizhzhia, Ukraine
oyn1973@gmail.com
https://orcid.org/0009-0000-9217-3619

CHAPTER 22.

Volodymyr SMIRNOV
Assoc. Prof., PhD tech. sci.
Central Ukrainian National Technical University,
Kropyvnytskyi, Ukraine
(8 Universytetskyi Ave, Kropyvnytskyi, Ukraine)
swckntu@gmail.com
https://orcid.org/0000-0002-4752-0527

Natalia SMIRNOVA
Assoc. Prof., PhD tech. sci.
Central Ukrainian National Technical University,
Kropyvnytskyi, Ukraine
(8 Universytetskyi Ave, Kropyvnytskyi, Ukraine)
swckntu@gmail.com
https://orcid.org/0000-0002-5683-5766

DOI 10.5281/zenodo.10820148
UDC 658.155:005.915

CHAPTER 1.
CRYPTO-ASSET TRANSACTION ARBITRAGE

Andrej LIPTÁK
Senior officer specialist Financial Investigation Department,
National Centre for Specific Crimes
Ministry of Interior of the Slovak republic
(Pribinova 2, 812 72 Bratislava, Slovak republic)
andrej.liptak@minv.sk
https://www.researchgate.net/profile/Andrej-Liptak/research

Abstract. Using qualitative and quantitative research methods, this study examines the principles and processes of crypto-asset transactions, identifying opportunities for transaction reversal and outlining methods to achieve this goal. The objective is to provide theoretical insights into addressing situations involving unwanted or unethical crypto-asset transactions, offering guidance to authorized entities, professionals, and the general public on preventive measures and corrective actions in the realm of crypto-asset-related crime. This contribution addresses the need to tackle current crypto-asset-related criminal activity, which encompasses a broad spectrum of illicit actions facilitated by crypto-assets. Unlike traditional fiat systems, where fiat currency serves as a means of exchange, crypto-assets offer an alternative. They not only enable the transfer of financially relevant information but also allow for the storage and immutable recording of data on a network, with automated tasks based on specified conditions. The article aims to offer theoretical knowledge and practical advice to authorized entities, law enforcement professionals, the professional and the general public regarding preventive measures and corrective actions in the realm of crypto-asset-related crime.

Keywords: crypto-asset, transaction, mempool, replacement, simulated transfer

Introduction and the problem statement. This contribution stems from the need to address the current state of criminality, which is characterized by the use of crypto-assets. This term is derived and will be used in this contribution based on Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance). Crypto-assets represent both an alternative to the commonly used financial system based on legal, institutional, and technological aspects, otherwise known as the fiat financial system. Where

financial assets of the fiat financial system, such as fiat currencies, can alternatively be represented by crypto-assets for the same purpose. In this sense, criminality related to crypto-assets is a very broad area, as wherever fiat currencies are used as a tool for committing criminal activities, as proceeds from criminal activities, as reward for the commission of a criminal offense, or as a bribe or motivation and incentive for committing criminal activities, crypto-assets can under similar conditions also be used. Therefore, crypto-assets cannot be considered solely as part of a specific type of criminality, as their scope is much broader. However, crypto-assets not only represent an alternative option for transferring financially relevant information. Crypto-assets enable the storage of individual pieces of information, i.e., data on the network, ensuring their immutability, allowing for the networked placement of logically ordered source code with automated task execution according to specified conditions. Certain types of criminal activities can also be conducted within the crypto-assets system, just as analogously on social networks or networks with a special access.

The subject of this contribution is, considering the current development of crypto-assets-related criminality in Slovakia and worldwide, to present, using methods and techniques of qualitative-quantitative research, the possibility of reversing a crypto-assets transaction. The term transaction evokes the transfer or movement of subjectively assessable values, which is too narrow a denomination concerning crypto-assets. The essence of a crypto-assets transaction is primarily the transfer and movement of data and information, and only when participants in the network assign financial character to this data can we regard a crypto-assets transaction as the transfer and movement of assessable values. However, in this contribution, we will abstract from any meaning of the term transaction other than this narrow essence of crypto-assets transaction. In this contribution, we analyze the basic principles of crypto-assets transactions, we dissect the process of constructing a transaction until its inclusion in a distributed transaction database. We identify the possibilities of reversing a crypto-assets transaction in the individual stages of this process and mediate the conditions, methods, and individual actions aimed at such reversal of a crypto-assets transaction.

The assumed result is the processing of a logically ordered aggregate, which will provide theoretical groundwork for acting prophylactically in the situation after the execution of an unwanted or reprehensible crypto-assets transaction. The purpose of the contribution is to highlight the possibilities of modification and recovery of assessable values in the form of crypto-assets if a crypto-assets transaction, for example, in fraudulent behavior, has already been initiated. The contribution answers the question: "What to do after executing a crypto-assets transaction that morally should not have been executed?". The aim of the contribution is to provide authorized enforcement agencies with a structure for implementing technical prophylactic measures in performing tasks defined by generally binding and internally related regulations; to the professional public, an insight into the issue of crypto-assets-related criminality in this specific and unusual area of execution and moral

manipulation with crypto-assets transactions; to the general public, guidance and options for proceeding in cases where unwanted crypto-assets transactions have been executed.

Foundation. Crypto-asset transactions involving financial relevant information can, under certain conditions, be analogously compared to transactions in the electronic fiat financial system, which are most commonly represented by electronic bank transfers of fiat currency funds. In the case of transferring fiat currency via electronic bank transfer, it is necessary for the initiator, i.e., the party authorized and having control to transfer fiat currency, to initiate such a transaction. The initiation of the transaction is often carried out through electronic banking applications, following proper registration and login, by entering the necessary details into a preset form, where the initiator must invariably provide the bank account identifier IBAN as the destination address, i.e., the recipient of the fiat currency, and the amount of fiat currency being transferred.

Confirmation of the information in the application form initiates the transaction by creating a request, which is then sent cryptographically from the application, and thus from the device where the fiat currency transaction was initiated, through the network to the banking institution for processing the desired transaction. The processing of the transaction is centralized and automated, with actions to verify the validity and truthfulness of the initiated fiat currency transaction, i.e., whether the initiator is an authorized holder of the sending fiat currency, or whether at the time of initiating the fiat currency transaction, they had a sufficient amount of fiat currency, etc. Often, after the initiation of the transaction, i.e., after the request is created and sent to the bank, this process becomes irreversible at this stage. The actual processing, realization, and confirmation of the fiat currency transaction take approximately several hours depending on the electronic banking services provided. Cancellation of such a fiat currency transaction is technically possible, but it requires the willingness of the banking institution to undertake immediate actions in favor of its client. Actions aimed at urgent cancellation of the transaction often involve additional fees and the necessity of visiting an institution branch, which includes providing explanations, filling out additional forms, and similar procedures. This, coupled with the time pressure resulting from the expected irreversible confirmation of the fiat currency transaction, presents a situation where failure is almost certain. After confirming such a fiat currency transaction, the banking institution, based on the details of the initiated fiat currency transaction, such as domestic transfer, international transfer, transfer between banking institutions, etc., processes the request for the return of fiat currency, which is then sent to the banking institution operating the recipient's IBAN. The processing time for domestic transfers is approximately 30 days, and for international transfers, it's approximately 180 days, with the actual return of fiat currency not guaranteed. The aforementioned information can be found on the website https://podnikam.sk/prevod-penazi-ako-prebieha-kolko-trva/.

Similar procedures apply to other financial institutions utilizing various payment methods that facilitate the transfer of financial assets or other assets electronically through data transmission.

Analogously, one can view crypto-asset transactions in a similar manner. To execute a transfer of crypto-assets, the transaction must be initiated. The initiation itself can be carried out either through a software interface, an application on a mobile device, or through specialized ATMs, known as crypto-assets ATMs or "crypto-ATMs," which handle the initiation of the transaction. This involves gathering the necessary input information for the transfer of crypto-assets, creating a request, encrypting it, and then sending it for processing. In comparison to the fiat currency bank transaction discussed earlier, there is a notable difference here. In the case of a sent request for processing and confirmation of a fiat currency transaction, it is addressed directly to the banking institution that registered the IBAN identifier for the initiator and often operates the application or software interface through which the fiat currency transaction was initiated. The process is characterized by centralization, meaning there is a single central authority - in this case, the chosen banking institution - that is present from the initiation of the transaction to its final confirmation.

However, the transfer of crypto-assets is a decentralized process, sometimes referred to by some authors as a distributed process. This means that the initiator of the transaction, whether he's using the application or crypto-ATMs, cannot process and confirm the transaction separately. In cases where the initiator of the crypto-assets transaction is also a network node responsible for processing and verifying the validity and truthfulness of the transaction (referred to as a "full node"), as well as a node in the network performing the activities of the consensus mechanism and recording information into the distributed transaction database (referred to as a "mining node"), and after meeting certain conditions gains the ability to record transactions into a block of transactions (known as mining a block), which is then added to the blockchain, and no other longer copy of the distributed transaction database exists, then it is possible for this initiator to both initiate and confirm such a crypto-asset transaction, which is considered relatively immutable.

The aforementioned request for processing a crypto-asset transaction is subsequently sent to entities responsible for verifying the correctness of the initiated transaction, whether it contains all the necessary elements for its confirmation, such as the correct format of the recipient's identifier for crypto-assets, i.e., the public address, which is the equivalent identifier to IBAN in the case of fiat currency transactions, and other details that will be addressed.

Furthermore, the truthfulness of the declared information in the initiated crypto-asset transaction is verified, such as whether the initiator possesses the crypto-assets they plan to send. This is verified by checking whether in the distributed transaction database, which contains only confirmed transactions, there is a sum of sent crypto-assets to the public address of the initiator that is at least equal to the amount the initiator plans to send to the recipient. After verifying the initiated crypto-

asset transaction and evaluating its validity, the transaction is marked as either satisfactory or unsatisfactory. Each device operates with a specific digital space referred to as device memory, where necessary digital records are performed. A transaction marked as unsatisfactory in the memory of such a device is labeled as over writeable, meaning that it is no longer relevant, and further action is not taken with it. On the other hand, a transaction marked as satisfactory is stored in the device's memory and awaits confirmation and inclusion into the distributed transaction database.

The confirmation of a crypto-asset transaction falls within the control of other nodes in the network, entities that, according to the network's rules, have the authorization to confirm this verified and valid crypto-asset transaction by including it in the distributed transaction database, or the so-called blockchain *(Šanta, J., Šanta, I., 2022)*, which represents the final handling of the crypto-asset transaction. The likelihood of immutability and integrity of the confirmed and recorded crypto-asset transaction is subsequently directly proportional to further subsequent confirmed transactions and thus with the passage of time. The temporal aspect from the initiation of the transaction to its confirmation and inclusion in the distributed transaction database is influenced by several factors. The most important objective factor is the type or kind of distributed transaction database, or the type of crypto-asset. In Table No. 1, we list 10 crypto-assets in descending order according to their traded value in terms of the equivalent in the US dollar. The provided data were obtained from the website "https://www.statista.com/statistics/944355/cryptocurrency-transaction-speed/" and the website "https://coinmarketcap.com/currencies/volume/monthly".

Table 1

Order	Crypto-asset	DLT (Distributed ledger technology)	Volume for December 2023 v USD	Transaction confirmation in minutes
1	Tether USDT	Ethereum Virtual Machine (EVM) - Tron	1 006 822 913 419	14-2
2	Bitcoin BTC	Bitcoin	540 528 857 257	40
3	Ethereum ETH	EVM	198 178 245 871	14
4	USDC	EVM	103 670 462 597	14
5	Solana SOL	Solana	56 173 143 728	1/60
6	First Digital USD FDUSD	EVM, Binance Beacon Chain (BNB Chain)	55 604 681 385	14-10
7	Binance Coin BNB	BNB Chain	31 241 791 015	10
8	SEI	Cosmos Atom	23 379 894 961	1/120
9	Wrapped Ether WETH	EVM	23 135 056 513	14

Order	Crypto-asset	DLT (Distributed ledger technology)	Volume for December 2023 v USD	Transaction confirmation in minutes
10	Internet Computer ICP	Internet Computer	18 884 333 797	1

On the surface, there exists an entity that, through a user-friendly interface, can easily execute fiat currency transactions or crypto-asset transactions after completing several steps. However, in the background, there are several tasks necessary for the proper initiation, packaging, encryption, sending, processing, verification, and subsequent confirmation of individual transactions. By understanding these component tasks, subsequent analysis can lead to theoretical and practical insights relevant to desired operations, such as in this case, the reversal of a crypto-asset transaction. *(Šanta, J., Šanta, I.,2023).*

The Mempool. Understanding the specifics of the transaction confirmation process for crypto-assets is essential in this regard. Initiated fiat currency transactions move data from the sender to the recipient in a centralized manner. Verification of whether the fiat currency transaction has been confirmed at the recipient's end can be confirmed by the sender by obtaining information from the entity executing the transaction confirmation, such as a banking institution. At that time, the sender only has information that the transaction was initiated and sent for processing and confirmation, primarily through an application or other software interface of electronic banking. It is recommended that access to this software interface be restricted to the sender, i.e., the account holder or authorized user associated with the account. The recipient of the fiat currency transaction receives confirmation information from the centralized banking entity only after the transaction is confirmed, typically through software interfaces of electronic banking linked to their account. By centralizing the transaction process, only the centralized entity has the information and capability to reverse such a fiat currency transaction.

In contrast, in the crypto-asset transaction system, information transfer is decentralized. Verification of a crypto-asset transaction sent by the initiator to the network is performed by decentralized entities, nodes in the network, or hardware-software interfaces designated for this purpose according to the rules of the crypto-asset. These nodes are characterized by maintaining a list of all crypto-asset transactions in their memory, which they receive and verify. This means that crypto-asset transactions are not verified by a single centralized entity that has the authority to control the original transaction list, but by many decentralized entities, network nodes, each of which possesses the original list of crypto-asset transactions. Of course, this raises doubts about the security of these crypto-asset systems because while the centralized fiat currency transaction system has an original transaction list in a much smaller number, increasing the risk of unwanted modification of this transaction list compared to the crypto-asset transaction system, where currently more than 10,000

entities possess this transaction list. However, on the other hand, the list of fiat currency transactions is much better protected in terms of physical, object, regime, administrative, and cybernetic security than the list of crypto-asset transactions, mainly because any device capable of basic data verification tasks can lead and thus be a node in the crypto-asset network.

After verification by multiple nodes in the network, the initiated crypto-asset transactions are considered verified but still unconfirmed and stored in a temporary storage of the node. This temporary storage is referred to as the "mempool," an abbreviation for "memory pool." The summary of transactions that the mempool can contain directly correlates with the size of the memory allocated within the hardware interface for storing verified but unconfirmed transactions. (*Florian, M., Beaucamp, S., Henningsen, S., Scheuermann, B. 2019*).

However, the confirmation of transactions lies within the competence of other network nodes equipped with sufficient computational power derived from their hardware-software setup to perform the mathematical and cryptographic operations necessary to confirm unconfirmed transactions and record them in the aforementioned list of all transactions. Transactions of crypto-assets recorded in this list of transactions are considered confirmed, and their reversal is deemed nearly impossible. The recording of a transaction, like the entire process of executing a crypto-asset transaction from initiation by the sender, is decentralized and thus transparent. A sender with sufficient technical capabilities can monitor this process throughout its duration. Those lacking such technical capabilities can rely on crypto-asset wallet service providers. In this regard, a crypto-asset wallet functions equivalently to an electronic banking application. However, as mentioned, the difference between the process of executing fiat currency and crypto-asset transactions lies primarily in decentralization and transparency, resulting in the fact that influencing the crypto-asset transaction process is sometimes easier than influencing the fiat currency transaction process. It is worth noting that crypto-asset transactions are recorded in the list of transactions in blocks, i.e., specific data files according to network rules. In the case of the Bitcoin network, these blocks are limited to 1 megabyte, sufficient to confirm approximately 3,000 transactions. Blocks of confirmed transactions in the Bitcoin network are recorded in the list of transactions approximately once every 10 minutes. As for unconfirmed crypto-asset transactions in the mempool, its size is naturally higher because confirmed transactions stem from unconfirmed ones, meaning the number of unconfirmed transactions awaiting recording can never be less than the number of confirmed and recorded transactions. *(Wang, K., Tong, M., Wu, CH., Pang, J., CHen, CH., Luo, X., Han, W. 2023.)*

The mempool is limited to approximately 300 megabytes, which equates to around 60,000 pending unconfirmed transactions. Upon recording a crypto-asset transaction into the list of all transactions, a node that has obtained authorization to record transactions into this list receives a reward in the form of crypto-assets in two ways. The first form entails the automatic release of crypto-

assets as per the network rules, which incentivizes network nodes to record crypto-asset transactions. The second form involves rewards derived from recorded transactions. The initiator of the transaction determines the reward associated with the crypto-asset transaction during its construction. This reward serves as a catalyst or inhibitor of the speed of the process of executing the crypto-asset transaction and its recording in the list of all transactions, which is the subject and commonly the purpose of the entire transaction process. In general, a verified unconfirmed crypto-asset transaction in the mempool is sorted according to the value of this predetermined reward. The higher the reward, the greater the likelihood that the transaction will be recorded in the list of all transactions sooner than those transactions with a lower set reward. This fact stems from the reality that the node recording transactions into the list of all transactions for crypto-assets utilizes economically costly hardware-software devices to generate the highest possible computational power, thus demanding the highest possible reward for recording a transaction. One form of reward is consistently dictated by the network rules, while the other form of reward is determined by the initiators of the transactions themselves, which are located in the mempool. The node recording transactions has the discretion to select from the total number of unconfirmed transactions in the mempool approximately 3,000 transactions that it has the right to record into the overall list of transactions.

Based on this, it is possible to some extent to predict the time when certain transactions will be recorded in the list of all transactions based on observing the values designated for nodes performing the recording of individual transactions in the mempool. The stability of the time prediction is primarily determined by the fact that the competition for transaction recording is extremely vast and demanding in terms of the overall computational power in the Bitcoin network, which is currently at approximately 500 million terahashes per second (TH/s), representing a value of around 8 billion USD for illustration, solely by the hardware interface designated for recording crypto-asset transactions. From this, it follows that the entities responsible for recording transactions into the list of transactions are significantly motivated to select from the mempool those unconfirmed transactions with the highest reward value.

The mempool is not rigid; the quantity of transactions cannot be precisely determined, especially considering the decentralized nature of the crypto-asset network. However, the same decentralization, along with the transparency of the network, ensures the availability of data and information that can be analyzed, measured, and quantitatively examined with a certain degree of predictive accuracy. It is worth mentioning that the number of unconfirmed transactions placed in the mempool is limited by the size of the mempool itself. If the mempool is full, it is unable to accommodate a larger number of transactions in its memory. In such cases, the mempool rejects these transactions and redirects them to another mempool, or deletes those crypto-asset transactions with a lower designated reward for the nodes performing the recording into the list, or database, of confirmed

transactions, and replaces them with those that have a higher included reward. The inclusion of a transaction into the mempool is a phase very close to the recording of the transaction into the list of all transactions. Transactions in the mempool are stored depending on the nature of other transactions in the network, typically for about 14 days. Automated prediction of transaction recording in the mempool can relatively reliably determine, at the time of the initial placement of the transaction into the mempool, whether and when the transaction will be confirmed during normal network operation. This assumption is based on a source available at the website "https://github.com/mempool/mempool.js".

This calculation and prediction can consensually consider the quality of a transaction, which, although unconfirmed, is initiated, verified, and meets all the conditions for inclusion in the list of all transactions, and given the current practice at the moment, which is mostly sufficient for network participants to consider this transaction as valid and behave towards it as if it were a completed transaction. In fact, the inclusion in the mempool and the determination of the expected time of recording, or the expected confirmation of the transaction, are so significant that crypto-asset wallet providers mediating simple user interfaces for their clients utilize this moment as sufficient evidence to inform the intended recipient of the crypto-assets about the received assets, even though the transaction has not been fully confirmed, i.e., it has not been actually recorded in the list of all crypto-asset transactions. It can thus be inferred that by manipulating the reward designated for nodes performing the recording into the list of confirmed transactions, one can influence the time required to confirm such a transaction. *(Mikhaylov, A., Dincer, H., Yuksel, S., Pinter, G., Shaikh, A. 2023.)*

Replacement of crypto-asset transaction. Based on the analyzed facts so far, it can be said that the process of executing crypto-asset transactions is transparent and decentralized, independent of any single entity, and is relatively observable in each of its partial phases. Independence also allows the initiator of a crypto-asset transaction to create, or initiate, multiple transactions arbitrarily. The verification of a crypto-asset transaction occurs only after its initiation, construction, and submission for verification. This means that the initiator has the ability to construct purposeful transactions. An example might be an unethical situation where the initiator, who is the controller of a certain amount of crypto-assets, perhaps having received 1 Bitcoin in a transaction in the past, which successfully went through the entire execution process and was duly recorded in the list of all transactions, therefore considered valid, constructs two transactions at one moment, both involving the transfer of 1 Bitcoin to two different recipients represented by two distinct public addresses.

Given the general nature of the network, nothing prevents both transactions from being considered acceptable to proceed with the process of executing crypto-asset transactions until proven otherwise. Due to the decentralization of the network, the initiator can send these transactions to different nodes for verification. Both transactions reference the same transaction history, which is

valid, so it's possible that both transactions will be independently marked as valid, verified, and included in the mempool. It's important to note that as these transactions progress through the execution process, the likelihood of one of them being rejected by the network diminishes. These already verified crypto-asset transactions, each separately included in two different mempools, are queued based on the reward designated for nodes performing transaction confirmation.

Even in such a highly unlikely scenario, which could be accelerated by offering high rewards to nodes performing transaction recording, where each transaction is independently recorded in the list of confirmed transactions by a separate node responsible for transaction confirmation, both transactions will be recorded in the list of all transactions and become confirmed. At this point, emphasized by the fact that crypto-asset wallet service providers have already notified the recipient about the received crypto-assets before the actual recording and confirmation of the transaction, a problem arises because the same crypto-assets with the same history have been spent twice, i.e., 1 Bitcoin has been spent twice. This could lead to infinite expansion of crypto-assets in an unethical manner, against the rules of the crypto-asset network.

Such a scenario is however rightly so, assumed by the network. From the initiation of the transaction to its recording in the list of all transactions, i.e., its confirmation, not even a few seconds may pass, especially if the initiator is knowledgeable, operates their own verification node, designates significantly high rewards for nodes performing transaction confirmation, or operates the confirmation node themselves and manages to obtain the right to record such transactions. To ensure the legitimacy of the list of all transactions for other participants, it needs to be shared among other network nodes. These nodes verify not only initiated transactions but also the entire list of recorded transactions and continuously monitor their validity.

If a record of all transactions containing both of these transactions, immoral but logically constructed, verified, and even logically recorded, were sent to the other nodes in the network, it would be rejected by the other nodes after subsequent, relatively quick verification. Not only would it be rejected, but the node that recorded this transaction would also be marked by the other nodes as a node attempting to manipulate the network, and they would no longer accept any information from it. Consequently, the node would lose the stable reward for transaction recording, as well as the reward from transactions designated by the transaction initiators that would otherwise be due to it. Additionally, it would lose the network's trust and essentially the ability to record transactions in the list of all transactions. This problem is known as double-spending, and it is essential to understand its nature and the measures taken by the crypto-asset network to address this issue, as its qualities can be exploited in replacing a transaction. *(Rondelet, A., Kilbourn, Q. 2023.)*

The results. By synthesizing the examined phases of crypto-asset transaction processes, technological aspects ensuring the execution of crypto-asset transactions, and knowledge gained from

comparing the system of executing crypto-asset transactions with the system of executing fiat currency transactions, it has been found that:

- The execution of crypto-asset transactions is governed by the rules of a decentralized and transparent network with constant monitoring capabilities of all phases of the crypto-asset transaction process.
- The execution of fiat currency transactions is governed by the rules of a centralized entity that oversees the entire process of executing fiat currency transactions.
- The process of executing both crypto-asset and fiat currency transactions occurs within a relatively short time frame, with the time frame for crypto-asset transactions being influenced by the determination of transaction fees.
- Reversing a fiat currency transaction is not practically possible after the transaction is constructed and sent for verification, processing, and confirmation.
- Reversing a crypto-asset transaction is possible by replacing it during the transaction verification and mempool inclusion phase, and under certain conditions, even after its confirmation.

Utilization for the purposes of simulated transfer. The results of the study should be presented on a modeled case, which represents a specific utilization of the method of crypto-asset transaction arbitrage. It is necessary to remind that this modeled case is just a small excerpt from the overall potential of arbitrage for individually targeted cryptocurrency transactions.

Simulated transfer, according to the Act No. 301/2005 Coll. – Criminal Code, Act No. 300/2005 Coll. – Penal Code (hereinafter referred to as the "Penal Code"), according to special legal regulations of the Slovak republic, and in accordance with criminal law theory, refers to simulating a purchase, sale, or other method of transferring the subject of fulfillment. This subject of fulfillment is conditioned by a special permit for possession, or its origin or purpose is causally linked to the commission of a criminal offense. Simulated transfer can be executed only after meeting the material and procedural conditions specified by currently valid and effective generally binding legal regulations. *(Marková, V., Strémy, T., Šanta, J., Janko, S., 2021).*

Modeled case. On January 15, 2024, an unknown attacker fulfilled the characteristics of a criminal offense according to § 189 of the Penal Code, para. 1 and para. 4 letter b) by threatening to erase data from the critical infrastructure institution's database, over which he gained electronic factual control, demanding ransom in the form of crypto-assets, by sending 50 Bitcoins to the provided public address representing the crypto-asset wallet (hereinafter referred to as the "perpetrator's wallet") within one hour, causing damage of approximately USD 2,000,000. Among other actions, a simulated transfer was promptly implemented as one of the means of operational-tracking activities. After securely setting up a unique state crypto-asset wallet (hereinafter referred to as the "state wallet") and obtaining 50 Bitcoins into the possession of the state wallet, the authorized

authority established the procedure for the simulated transfer. The construction of the transaction, where the initiator of the transaction would be the public address of the state wallet, the recipient the public address of the perpetrator's wallet, a sum of 50 valid and legitimately obtained Bitcoins, and transaction fees, i.e., rewards for nodes securing the confirmation of crypto-asset transactions at such a level that the transaction would be ranked in the mempool queue so that the crypto-asset transaction would not be confirmed and recorded in the list of all transactions immediately, but at the same time, it would not be removed from the mempool. Removing the transaction from the mempool could lead to a loss of information in the network, which the perpetrator could interpret as a failure to comply with his request and thus to the subsequent deletion of the critical infrastructure institution's data database. Confirmation and recording of the transaction in the list of all transactions would comply with the perpetrator's request, thereby not achieving the purpose of executing the simulated transfer. To determine the most ideal value of transaction fees, the mempool of all available nodes was analyzed, and a calculated presumable prediction was made. The next step was to create a second public address of the state wallet and construct an arbitrage transaction of crypto-assets, consisting of the initiator, which was the first public address of the state wallet, the recipient, which was the second public address of the state wallet, a sum of 50 Bitcoins, and transaction fees high enough so that after placing the arbitrage transaction into the mempool along with the original transaction, there would be a significant preference for confirming the arbitrage transaction. The actual execution of the simulated transfer consisted of sending the original crypto-asset transaction with optimized fees to the public address of the perpetrator's wallet, notifying the perpetrator of the construction of the crypto-asset transaction, and requesting access to the critical infrastructure institution's database. After notifying the perpetrator about the constructed transaction, crypto-asset related facts were monitored in the network, and it was found that the crypto-asset transaction was included in the mempool, which was enough to pursue the access the data from the critical infrastructure institution's database. After analyzing this data, the data was immediately backed up, followed by the immediate sending of the arbitrage crypto-asset transaction, which surpassed the original transaction in the mempool and was confirmed and recorded in the list of all transactions before the original transaction. Due to double-spending measures, the original transaction was rejected and removed from the mempool, resulting in gaining access to the data from the critical infrastructure institution and returning the 50 Bitcoins.

The terminology used in concurrence to study done by Ján Šanta and Ivan Šanta. (*Šanta, J., Šanta I., 2023).*

Conclusion. Reversing a fiat currency transaction is contingent upon necessary cooperation and collaboration with centralized entities that guarantee and secure the fiat financial system, given the centralized nature of the transaction process. Reversing such a transaction occurs by halting the flow of data, thereby interrupting the automated procedures resulting from the hardware-software

interface used in initiating or further processing the transaction. The flow of data, which has left one centralized entity, where the software interface, such as internet banking, is often managed, does not possess the authority and technical capability to interrupt this flow of data and thus prevent the transaction from being executed. Up to this point, very close and very prompt cooperation with this entity is necessary, which is associated with performing a multitude of administrative and bureaucratic tasks. The likelihood of reversing a fiat currency transaction after its initiation and sending from the software interface of the initiating entity to the entity ensuring the verification and confirmation process of the transaction is highly improbable.

Reversing a crypto-asset transaction is contingent upon one's own knowledge and abilities, given the decentralized and transparent nature of the transaction process, whereby the transaction flow can be influenced until the transaction is recorded in the distributed transaction database, which is generally considered an irreversible moment and thus the final processing of the transaction. Up to this point, a crypto-asset transaction can be replaced by manipulating the fees designated for nodes responsible for recording the transaction in the distributed transaction database, i.e., the list of all confirmed crypto-asset transactions. By initiating a copy of the transaction early, where there is an interest in its replacement and therefore cancellation, while simultaneously increasing the fees for the mentioned nodes, there is a preference in the crypto asset-network, usually in the mempool, for the copy of the transaction, despite the fact that the original transaction with the same history was initiated, constructed, and verified earlier from a time perspective. The timeframe for possible manipulation of transactions depends on the determination of fees in the original transaction, whereby it holds that the smaller the fees for the mentioned nodes in the original transaction, the more time is needed for its final confirmation, which also creates more time for its reversal, but it also depends on the type of crypto-asset used, depending on the speed of the entire processing and confirmation process of the transaction of that crypto-asset.

These facts can be prophylactically utilized in the legitimate activities of authorized entities, as well as by any initiators of crypto-asset transactions who meet the conditions of asymmetric cryptography of the given crypto-asset system.

References:

ŠANTA, J., ŠANTA, I. (2023). Virtuálne meny - trestnoprávne a niektoré analyticko-ekonomické aspekty. Praha: Leges, 2023. 199 strán. ISBN: 978-80-7502-668-2

MARKOVÁ, V., STRÉMY, T., ŠANTA, J., JANKO, S. (2021). Trestné právo procesné. Všeobecná časť. Plzeň: Aleš Čeněk, 2021. 363 s. ISBN 978-80-7380-861-7

ŠANTA, J., ŠANTA, I.. (2023). K najaktuálnejšej počítačovej a inej kriminalite súvisiacej s virtuálnymi menami In: Justičná revue. – Roč. 75, Vydanie 5/2023, s. 636 – 650. ISSN 1335-6461 (tlačené vydanie)

ŠANTA, J., ŠANTA, I. (2022). Riziká investovania do virtuálnych mien z ekonomického a trestnoprávneho hľadiska. In: Justičná revue. – Roč. 74, Vydanie 3/2022, s. 365 – 378. ISSN 1335-6461 (tlačené vydanie)
WANG, K., TONG, M., WU, CH., PANG, J., CHEN, CH., LUO, X., HAN, W. (2023). Exploring Unconfirmed Transactions for Effective Bitcoin Address Clustering. *Cryptography and Security (cs.CR),* 2023. https://doi.org/10.48550/arXiv.2303.01012
MIKHAYLOV, A., DINCER, H., YUKSEL, S., PINTER, G., SHAIKH, A. 2023. Bitcoin mempool growth and trading volumes: Integrated approach based on QROF Multi-SWARA and aggregation operators. *Journal of Innovation & Knowledge,* vol. 8, no. 3, (2023). https://doi.org/10.1016/j.jik.2023.100378
RONDELET, A., KILBOURN, Q. 2023. Mempool Privacy: An Economic Perspective. *Cryptography and Security (cs.CR).* (2023). https://doi.org/10.48550/arXiv.2307.10878
FLORIAN, M., BEAUCAMP, S., HENNINGSEN, S., SCHEUERMANN, B. 2019. Erasing Data from Blockchain Nodes. *IEEE Security & Privacy on the Blockchain (IEEE S&B), 2019.* https://doi.org/10.48550/arXiv.1904.08901
Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance)

DOI 10.5281/zenodo.10820221
UDC 338.48-44(1-87)

CHAPTER 2.
THE ESSENCE OF THE CONCEPT OF "TOURISM POLICY" AND INTERNATIONAL MODELS OF ITS IMPLEMENTATION

Nadiya BAKALO
PhD (Economics), Associate Professor,
Associate professor international economic relations and tourism department
National University «Yuri Kondratyuk Poltava Polytechnic»
(Poltava, Pershotravnevaya avenue, 24, Ukraine)
bakalo.nv@ukr.net
https://orcid.org/0000-0002-3260-412X

Viktoriia MAKHOVKA
PhD (Economics)
National University «Yuri Kondratyuk Poltava Polytechnic»
(Poltava, Pershotravnevaya avenue, 24, Ukraine)
mahovkavm@gmail.com
https://orcid.org/0000-0001-7985-7792

Abstract. The monograph examines the essence and features of the concept of "tourist policy" and international models of its implementation; peculiarities of the formation of tourism policy in the countries of the European Union and the prospects of using their experience in Ukraine. It is established that during the last decade, important transformations in the field of tourism have been noted, which are caused by socio-economic and political changes. It was noted that one of the important forms of international legal regulation and coordination of the state's activities in the field of tourism are UN conferences on tourism, UNWTO conferences, and forums of international tourism organizations. We considered the positive experience of the development of the following member states of the European Union, such as Poland, France, Hungary, Slovakia, the Czech Republic, Italy, Spain, Portugal, Greece, Monaco, and Bulgaria. Having conducted an analysis of the experience of state administration in the formation of the tourism potential of these countries, they drew conclusions and provided suggestions regarding the application of this experience in Ukraine.

Keywords: tourist policy; foreign experience; international tourist organizations; tourist potential.

СУТНІСТЬ ПОНЯТТЯ «ТУРИСТИЧНОЇ ПОЛІТИКИ» ТА МІЖНАРОДНІ МОДЕЛІ ЇЇ РЕАЛІЗАЦІЇ

Анотація. В монографії розглянуто сутність та особливості поняття «туристичної політики» та міжнародні моделі її реалізації; особливості формування туристичної політики в країнах Європейського Союзу та перспективи використання їх досвіду України. Встановлено, що упродовж останнього десятиліття відзначаються важливі трансформації в сфері туризму, які обумовлені соціально-економічними та політичними змінами. Зазначили, що однією з важливих форм міжнародно-правового регулювання та координації діяльності держави у сфері туризму є конференції ООН з туризму, конференції UNWTO, та форуми міжнародних туристичних організацій. Розглянули позитивний досвід розвитку наступних країн-членів Європейського союзу як Польщі, Франції, Угорщині, Словаччині, Чехії, Італії, Іспанії, Португалії, Греції, Монако, Болгарії. Провівши аналіз досвіду державного управління у формуванні туристичного потенціалу даних країн зробили висновки та надали пропозиції, щодо застосування цього досвіду в Україні.

Вступ. Формування туристичної політики в країнах Європейського Союзу визначається не лише економічними вигодами, але і культурними та соціальними аспектами. З огляду на багатий культурний спадок та різноманітність природних ресурсів, європейські країни вдаються до цілеспрямованих стратегій та підходів для приваблення туристів, забезпечуючи при цьому сталість та баланс у розвитку туристичної галузі. Однією з важливих складових формування туристичної політики ЄС є спрямованість на сталий розвиток. Країни акцентують на розумному використанні ресурсів, збереженні природного середовища, та взаємодії з місцевим населенням для максимізації позитивного впливу туризму на економіку та культурне спадщину. Культурна різноманітність Європейського Союзу створює особливий контекст для формування туристичних програм та подорожей. Привабливість історичних пам'яток, мистецтва, архітектури, традиційної кухні та фестивалів визначається уважним врахуванням цих аспектів у туристичних стратегіях.

За останні десятиріччя країни ЄС виявилися лідерами у розвитку туризму, впроваджуючи інноваційні підходи, спрямовані на збереження культурної спадщини, підтримку сталого розвитку та створення зручного середовища для туристів. Однак, незважаючи на власний потенціал, Україна може використати досвід від країн ЄС у вдосконаленні маркетингових стратегій, розвитку інфраструктури, та ефективного управління

туристичним потоком. У цьому контексті, аналіз та адаптація найкращих практик країн Європейського Союзу стає важливим етапом для України на шляху до формування інноваційної та конкурентоспроможної туристичної політики. У даному вступі розглянемо основні напрями та принципи, які можна взяти на озброєння з європейського досвіду для досягнення стратегічних цілей у сфері туризму в Україні.

Розділ 1. Сутність поняття «туристичної політики» та характеристика її рівнів

Поява такого поняття як «політика» відоме з часів стародавньої Греції, його активно використовували відомі філософи Платон і Аристотель. У сучасній лексиці це слово з'явилося як запозичення з грецької мови і традиційно вказує на діяльність, яка пов'язана з управлінням та відносинами між особами, соціальними групами, народами, націями та державами в контексті справ громадського та державного характеру (*Австрійський національний туристичний офіс*).

Упродовж останнього десятиліття відзначаються важливі трансформації в сфері туризму, які обумовлені соціально-економічними та політичними змінами. Туризм є важливою галуззю з високими прибутковими можливостями, які забезпечують високий рівень зайнятості, соціального добробуту та підвищення якості життя населення. Це ключовий сектор світової економіки, який сприяє розвитку держави і регіонів, сприяючи їх єдності та культурному різноманіттю.

Держави роблять акцент на досягнення максимальної вигоди від туристичної галузі, розвиваючи відповідну інфраструктуру (таку як транспортну інфраструктуру, парки, заклади розміщення та харчування, сферу торгівлі тощо) та створюючи нові робочі місця.

Проведені дослідження свідчать, що термін «туристична політика» не має чіткого визначення в спеціалізованих виданнях, але він широко використовується в академічних дослідженнях, навчальних матеріалах та програмах навчання. Розглянемо сутність поняття «туристична політика» на рис. 1.

Герасименко В. Г. [3]

- Система методів, впливів і заходів соціально-економічного, правового, зовнішньополітичного, культурного й іншого характеру, яка здійснюється парламентами, урядами, державними і приватними організаціями, асоціаціями і закладами, що відповідають за туристичну діяльність, з метою регулювання і координації туристичної галузі, створення умов для розвитку туризму.

Любіцева О. О. [6]

- Державна туристична політика є комплексом заходів правового, економічного і організаційного порядку, підкріплена відповідними управлінськими інститутами, діяльність яких пронизує всі управлінські рівні і спрямована на узгодження державних, бізнесових і місцевих інтересів на ринках туристичних послг різного порядку.

Михайліченко Г. І. [8]

- Державна туристична політика – система методів і заходів економічного, політичного, соціального, правового, культурного характеру, що здійснюється як державними, так і недержавними органами, відповідальними за туристичну діяльність.

Рис. 1. Сутність поняття «туристична політика»

У науковій літературі можна знайти різноманітні визначення політики держави у сфері туризму, і кілька з них подано на рис. 1, проте незважаючи на їх схожі риси, між цими визначеннями є ряд відмінностей, які відображають різні тлумачення суб'єктів, об'єктів та цілей державної туристичної політики.

Мета державної туристичної політики полягає у забезпеченні ефективного використання туристичних ресурсів, розробці стратегічних планів щодо туристичного розвитку для запобігання можливим серйозним екологічним та соціокультурним проблемам, підтримці покращення стану навколишнього середовища та задоволення високих потреб туристів, одночасно зберігаючи привабливість місць як туристичного напрямку.

Туристична політика може бути організована на різних рівнях управління, включаючи національний, регіональний, місцевий і міжнародний рівні. Рівні туристичної політики визначаються на основі того, хто приймає рішення та здійснює дії в галузі туризму. Зазвичай, виділяють такі основні рівні туристичної політики:

1. Міжнародний рівень: коли справа стосується міжнародного туризму і співпраці між країнами, міжнародні організації, такі як Всесвітня організація туризму (UNWTO), можуть встановлювати стандарти і рекомендації для країн та сприяти обміну інформацією і найкращими практиками.

2. Національний рівень: національна туристична політика визначається урядом країни і спрямована на регулювання розвитку туризму на всій території країни. Вона включає в себе визначення стратегічних цілей, фінансові стимули, регулювання галузі, маркетинг та рекламу, а також співпрацю з іншими країнами та міжнародними організаціями.

3. Регіональний рівень: в деяких країнах туристична політика може бути розроблена і реалізована на регіональному рівні, де регіональні адміністрації або автономні регіони встановлюють власні стратегії та ініціативи для розвитку туризму на своїй території.

4. Місцевий рівень: органи місцевої влади, такі як міські адміністрації та районні органи, також можуть розробляти і виконувати свої власні туристичні стратегії та програми. Це може включати в себе розвиток конкретних туристичних атракцій та послуг, місцевий маркетинг та рекламу (*Герасименко В.Г., 2008*).

Вищевказані рівні туристичної політики можуть взаємодіяти і співпрацювати між собою для досягнення загальних цілей, але вони також мають власні компетенції та завдання. Розуміння рівнів туристичної політики допомагає краще координувати зусилля між різними рівнями влади для підтримки розвитку туризму.

Вибір об'єктів та цілей туристичної політики значною мірою залежить від рівнів, на яких ця політика реалізується. Такий підхід до туристичної політики охоплює від міжнародного та національного рівнів до регіонального і місцевого.

Кожен із цих рівнів акцентує увагу на різних деталізаціях цілей, враховуючи особливості кожного з рівнів. В ідеалі процес реалізації туристичної політики має починатися із загальних принципів і поступово розгортатися до конкретних заходів і рішень на різних рівнях.

На міжнародному рівні туристична політика формується міжнародними організаціями, такими як Всесвітня організація туризму (UNWTO), Об’єднана федерація асоціацій туристичних агентств, Міжнародна асоціація готелів та ресторанів, Всесвітня рада туризму і подорожей, Міжнародна асоціація повітряного транспорту та інші подібні організації (*Ключик Р.М., 2020*).

Звісно, основною метою UNWTO, провідної міжнародної організації в галузі туризму, є сприяння сталому розвитку туризму для досягнення економічного, соціального та культурного піднесення суспільства, боротьби з бідністю та забезпечення світу. UNWTO розробляє загальні принципи розвитку міжнародного туризму, займається питаннями міжнародного співробітництва в галузі туризму, створює правові основи для нього, гарантує безпеку та доступність подорожей, звертає увагу на екологічні аспекти безпеки та стандартизує якість туристичних послуг та багато іншого.

Регіональна стратегія в галузі туризму базується на основних принципах національної туристичної політики та відображається в програмах розвитку туризму на регіональному рівні, які розробляються з урахуванням конкретних умов і завдань розвитку конкретних територій.

Національна туристична політика має своїм основним завданням розробку принципів, створення рамкових умов та визначення стратегічних напрямків розвитку сфери туризму. Ця політика створюється через концепцію та цільові програми розвитку туризму та створює шляхи їх впровадження. Важливо, щоб вона сприяла формуванню основи для впровадження регіональної туристичної політики (*Хорватська національна туристична рада*). В табл. 1 представлено рівні та завдання туристичної політики.

Таблиця 1.

Рівні та завдання туристичної політики

Рівень туристичної політики	Завдання
Національний рівень:	– розробка національних стратегій і політик у сфері туризму. – регулювання та контроль за ринком туристичних послуг і підприємств. – вивчення і аналіз потоків туристів та їх впливу на економіку та суспільство. – встановлення стандартів та правил для туристичної галузі. – приваблення іноземних туристів та інвестицій.
Регіональний рівень:	– розвиток регіональних стратегій та програм для збільшення туристичного руху. – просування інфраструктурного розвитку на регіональному рівні. – співпраця з місцевими органами влади та громадами для забезпечення підтримки туризму. – організація рекламних кампаній та заходів для приваблення туристів на регіональний рівень.
Місцевий рівень:	– розвиток інфраструктури для туристів, таких як готелі, ресторани та транспортні послуги. – забезпечення безпеки і комфорту для туристів на місцевому рівні. – просування культурних та природних атракцій на місцевому рівні. – залучення місцевого громадськості та підприємців до розвитку туризму
Міжнародний рівень:	– участь у міжнародних туристичних організаціях та обмін інформацією з іншими країнами. – розвиток міжнародних маркетингових кампаній для приваблення іноземних туристів. – участь у міжнародних стандартах і регулюванні туризму.

Джерело: побудовано автором на основі (*Хорватська національна туристична рада*)

Основи міжнародно-правового регулювання системи туризму і міжнародних подорожей закладено у низці міжнародних договорів, актів, конвенцій і декларацій міжнародних організацій, які є головними інструментами регулювання міжнародної туристичної діяльності.

Основні міжнародні акти, що безпосередньо регулюють туристську діяльність представлені на рис. 2.

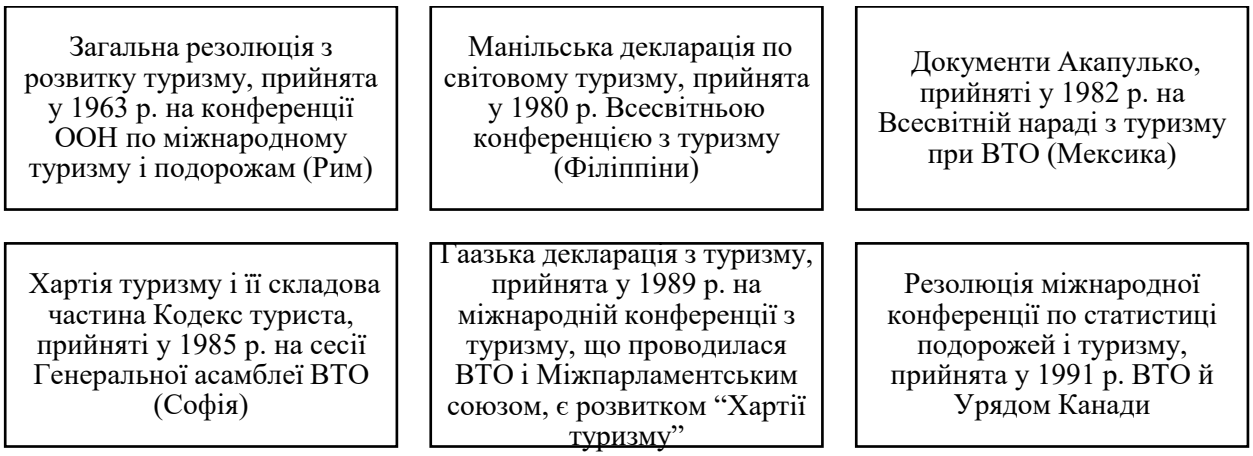


Рис. 2. Основні міжнародні акти, що безпосередньо регулюють туристську діяльність

Джерело: побудовано автором на основі (*Хорватська національна туристична рада*)

Основні заходи для координації та регулювання туристичної діяльності включають діяльність конференцій, асамблеї, зустрічі, форуми, конгреси, та семінари, які організовані міжнародними установами.

Однією з важливих форм міжнародно-правового регулювання та координації діяльності держави у сфері туризму є конференції ООН з туризму, конференції UNWTO, та форуми міжнародних туристичних організацій (*Sürdürülebilir Turizm/ Sustainable Tourism. Rapor, Eylül*).

Для глобальної економіки характерно і створення організаційних структур управління на міжнародному рівні, що відноситься і до галузі міжнародного туризму. Постійне зростання та розвиток міжнародного туристичного обміну породжує необхідність його регулювання на міжнародному рівні через введення різноманітних правових інститутів і створення спеціалізованих туристичних організацій.

Туристичні організації можна класифікувати за такими ознаками:

– національно-територіальна (міжнародні, регіональні та національні туристичні організації;

– їх діяльність має світовий, регіональний та національний характер);

– суспільно-державна (урядові, громадські, приватні);

– вид діяльності (регулюючі, постачальники, ринкові агенти, розробники, консультанти, проектні організації, навчальні організації, видавці, професійні асоціації, торгівельні та споживацькі організації);

– сфера діяльності (транспортні (авіаційні, автобусні, залізничні, автомобільні і круїзні), туристичні агенти, туроператори, локальні профспілки) (*Бойко М., Гопкало Л., 2005*).

Основними міжнародними організаціями є: Всесвітня туристична організація, Міжнародна асоціація повітряного транспорту, Міжнародна організація цивільної авіації. Реалізація наддержавного регулювання в сфері туризму на регіональному рівні здійснюється регіональними організаціями. Основні з них: Організація економічного співробітництва та розвитку, Азіатсько-Тихоокеанська туристична організація.

– Розглянемо світовий досвід державного регулювання туристичної діяльності. М. Бойко розглядає чотири моделі управління туристичною сферою країни (рис. 3) (*Бойко М., Гопкало Л., 2005*).

Перша (ринкова) модель

- передбачає відсутність центральної державної туристичної адміністрації, органу державного управління на рівні центральної влади.

Друга модель розвитку туризму

- передбачає наявність спеціального, потужного, авторитетного й самостійного державного центрального органу - міністерства, що займається розвитком й контролює діяльність усіх підприємств туристичної галузі в країні.

Третя (європейська) модель

- передбачає, що питання розвитку туристичної діяльності на рівні відповідного галузевого підрозділу, який функціонує в рамках багатофункціональних міністерств або напряму підпорядковується урядові країни.

Четверта (комбінована) модель

- передбачає створення комбінованого міністерства, але, крім туризму охоплює інші, суміжні з ним або взаємодоповнюючі напрями соціально-економічної політики.

Рис. 3. Чотири моделі управління туристичною сферою країни

Перша (ринкова) модель передбачає відсутність центральної державної туристичної адміністрації на рівні центральної влади. У цій моделі всі аспекти, пов'язані з розвитком туризму, розглядаються і вирішуються на рівні регіонів або незалежно суб'єктами господарювання. Це відбувається на основі оперативного регулювання та принципів ринкової економіки. Основною умовою для застосування цієї моделі є те, що країна повинна бути привабливою для іноземних туристів з усіх аспектів і не потребувати спеціальної реклами національного туристичного продукту на світовому ринку.

Така модель управління туристичною сферою була розроблена в США, де з метою економії бюджетних коштів у 1997 р. була ліквідована державна структура U.S. Travel and Tourism Administration (USTTA), що відповідала за розвиток туризму в країні. Це було зумовлено тим, що США здатні витримати міцні позиції на міжнародному туристичному ринку, а сильні приватні компанії спроможні на самостійні рекламні заходи в інтересах усього національного ринку туризму. Замість USTTA в США діє Консультативна рада з туризму та

подорожей (USTTAB) – досить впливовий орган, до складу якого входять значні представники туристичної індустрії.

Однак, прийняття першої моделі можливе лише у випадках, коли туризм національній економіці взагалі не потрібний або коли суб'єкти туристичного ринку настільки сильні та свідомі, що здатні вирішувати всі свої проблеми без участі держави. Такий підхід ефективний у країнах з розвинутою ринковою економікою, де переважають приватні компанії різної величини та спеціалізації. Важливе значення при цьому мають розвинена інфраструктура, система забезпечення безпеки туристів, високий рівень надання банківських, страхових послуг і медичного обслуговування.

Друга модель розвитку туризму передбачає наявність спеціального, потужного, авторитетного й самостійного державного центрального органу – міністерства, що займається розвитком й контролює діяльність усіх підприємств туристичної галузі в країні. Міністерство має значні повноваження у сфері інвестицій, маркетингових досліджень, підготовки кадрів, реклами тощо. Спеціалізовані органи займаються майже виключно питаннями функціонування туристичної галузі.

Така модель управління туристичною індустрією властива багатьом країнам, що розвиваються, країнам з перехідною економікою, для яких туризм є одним з основних джерел валютних надходжень у бюджет, а також деяким високорозвиненим з туристичного погляду держави, які мають намір постійно підтримувати на належному рівні туристичний імідж. У цих країнах туризму надається важливе значення в державній туристичній політиці. Для реалізації такого підходу необхідні визначені умови, зокрема: великі фінансові інвестиції в туристичну галузь для розробки та утримання національного туристичного продукту та туристичної інфраструктури, забезпечення підтримки держави для малого та середнього бізнесу, створення ефективної системи безпеки для туристів і таке інше.

Третя (європейська) модель переважає в розвинених європейських державах. Вона передбачає, що питання розвитку туристичної діяльності на рівні відповідного галузевого підрозділу (централізована структура, державний орган), який функціонує в рамках багатофункціональних міністерств (найчастіше економічного спрямування) або напряму підпорядковується урядові країни, однак має статус відносно самостійного адміністративного органу.

У різних країнах світу спеціалізовані галузеві підрозділи (урядові або напіврядові) називаються по-різному, але за сутті все вони є Національними туристичними адміністраціями (НТА), до компетенції яких належить формування державної туристичної політики.

– Характерними рисами даного типу розвитку туризму є: погодження інтересів держави, місцевої влади та приватного бізнесу; взаємовигідні форми співробітництва між органами управління макроекономічного та мезоекономічного рівнів; у країнах діють багато інших організацій, що займаються питаннями розвитку туризму (перебувають в адміністративному упорядкуванні у вищезгаданих структур або функціонують автономно). Така схема роботи виявилася досить продуктивною для залучення фінансових засобів приватного сектору до вирішення актуальних завдань розвитку національної економіки (*Бойко М., Гопкало Л., 2005*).

Четверта (комбінована) модель розвитку туристичної галузі передбачає створення комбінованого міністерства, але, крім туризму охоплює інші, суміжні з ним або взаємодоповнюючі напрями соціально-економічної політики. За даними Всемірної туристичної організації, у понад 80 країн світу туризм переважно віднесено до компетенції міністерств і відомств економічного блоку (міністерства економіки, торгівлі, транспорту, промисловості, фінансів), решта – до міністерств та відомств соціального блоку (міністерства культури, екології, освіти, інформації, археології (*Домбровська С.М., Білотіл О.М., Помаза-Пономаренко А.Л., 2016*).

Для країн, які дотримуються такого типу державного регулювання, характерним є визначення туризму як пріоритетного напряму економічного розвитку, що досягається чітким розподілом повноважень між центральною та регіональною адміністрацією. Основними цілями державної туристичної політики таких спільних міністерств є забезпечення збалансованості розвитку туризму та інших галузей економіки, а також просування національного туристичного продукту за кордоном. Ця модель поєднує в собі другу і третю моделі розвитку індустрії туризму. Він знайшов широке застосування в тих країнах, які мають намір позиціонувати себе як сприйнятливі туристичні ринки.

Розділ 2. Особливості формування туристичної політики в країнах Європейського Союзу та перспективи використання їх досвіду України

Алгоритм управління сферою туризму відрізняється в різних країнах та залежить від економічної ролі туризму в них. Це пов'язано з унікальними природними та історико-культурними ресурсами, потенціалом національного туристичного ринку, доступністю туристичних ресурсів для внутрішніх і міжнародних туристів, а також роллю країни на світовому туристичному ринку, обсягами інвестицій у туризм та іншими факторами.

Важливо зауважити, що управління туристичною галуззю кожної країни різниться в залежності від рівня розвитку держави, економічної ролі туризму, обсягів інвестицій у туристичну сферу та інших аспектів. Навіть наявність значного туристичного потенціалу не

може гарантувати успішний розвиток туристичної індустрії, оскільки для цього необхідне ефективне державне управління туристичною галуззю.

Основною нашою метою є виявлення особливостей державного управління процесом формування туристичного потенціалу країн Європейського союзу та пошук можливостей імплементації цього досвіду в Україні. Ми вивчили досвід наступних країн-членів Європейського союзу як Польщі, Франції, Угорщині, Словаччині, Чехії, Італії, Іспанії, Португалії, Греції, Монако, Болгарії. Тому далі ми розглянем позитивний досвід кожної з цих країн і як саме його можна використати для удосконалення туристичної політики України.

Україна може здобути корисний туристичний досвід, орієнтуючись на Польщу, так як вона є найбільш близькою за аналогією. Польща, аналогічно до України, володіє різноманітними туристичними ресурсами. Обидві країни спільно організували Європейський чемпіонат з футболу «Євро-2012», внаслідок чого вже існує позитивний досвід у сфері туристичного співробітництва між державами. Україна може застосовувати досвід Польщі у розвитку та підвищенні привабливості внутрішнього туризму, зокрема шляхом використання потенціалу туристичних ресурсів.

В Польщі функціонує приблизно 70 тисяч готельних закладів (*Robinson Peter, Lück Michael, Smith Stephen L. J., Lackey Michael., 2013*), які взаємодіють із закладами ресторанного господарства, транспортними компаніями та іншими об'єктами. Інфраструктурні туристичні ресурси включають аквапарки, зоопарки, торгово-розважальні комплекси, тощо.

Польща входить до десятки найбільш відвідуваних країн іноземними туристами. На її курортах створено сприятливі умови для лікування та відпочинку. Країна реалізує ефективну державну політику у сфері туризму, базуючись на належному нормативно-правовому та інституційному забезпеченні.

Усі туристичні права та обов'язки суб'єктів туристичної галузі закріплені в Конституції Польщі (*Robinson Peter, Lück Michael, Smith Stephen L. J., Lackey Michael., 2013*). Важливо відзначити, що успіх Польщі у сфері туризму обумовлений не лише розвитком туристичних компаній та підтримкою міністерства, а також зусиллями представників органів місцевого самоврядування.

Туристичний ринок Польщі протягом останніх двадцяти років розвивається із значно вищою інтенсивністю, порівняно з українським. Сильний туристичний потенціал країни створює сприятливі умови для формування високорозвиненого та прибуткового курортно-рекреаційного господарства, особливо в курортно-туристичних регіонах. До передумов цього розвитку відносяться:

1. Руйнування старої системи і створення Польської туристичної палати, що представляє інтереси своїх членів у сфері туризму.

2. Скасування віз для громадян Польщі до багатьох країн Європи.

3. Реалізація Програми розвитку національного туристичного продукту в п'яти напрямах: бізнес-туризм, міський культурний туризм, сільський туризм, спеціалізований туризм, прикордонно-транзитний туризм.

4. Створення позитивного іміджу польського туристичного продукту в державі та за її межами, активний розвиток інформаційної мережі та участь у програмах розвитку туристичної індустрії та модернізації інфраструктури.

5. Вступ до Європейського союзу, що зробив Польщу більш доступною для іноземних туристів, усуваючи митні та прикордонні бар'єри.

6. Реалізація екологічних програм, розбудова курортних закладів, готельних ланцюгів, модернізація туристичних маршрутів, гірськолижних витягів і т.д.

7. Співпраця з численними інституціями та організаціями.

8. Організація освітніх подорожей для польських та іноземних журналістів і інфотурів для туроператорів, спрямована на презентацію об'єктів з великим туристичним потенціалом. Це сприяє популяризації польського туристичного продукту в медіа та розширенню вибору пропозицій щодо відпочинку в Польщі.

Просування туризму в Польщі здійснюється завдяки підготовці, друку рекламно-інформаційних матеріалів, моніторингу ринків різних країн відповідно до їхнього розташування, проведенню рекламних кампаній та заохоченню потенційних партнерів до співпраці. Ці матеріали випускаються дванадцятьма мовами і надають потенційним туристам необхідну інформацію. Завдяки характерному дизайну і змістовному наповненню, ці друковані матеріали визнані одними з найкращих у світі.

Активна туристична політика Польщі, відповідно до даних Всесвітньої туристичної організації ООН (ЮНВТО), призводить до позитивної динаміки туристичних прибутків і надходжень, роблячи її цікавим прикладом для віддзеркалення у діяльності відповідних українських органів влади. Для розробки конкретних рекомендацій з практичною спрямованістю доцільно впроваджувати додаткові дослідження у цьому напрямку, аналізуючи кожен аспект реалізації туристичної стратегії окремо. Також буде корисно ініціювати національні програми обміну досвідом для керівників галузі та використовувати успіхи Польщі в цьому відношенні.

Особливо цікавим є проект Польщі «Туризм для всіх», що втілюється через створення в інтернеті бази даних про доступність туристичної інфраструктури для туристів з особливими

потребами. В туристичному бізнесі Польщі розуміють, що важливо зробити все можливе, щоб турист захотів повертатися в цю країну. Багато польських туристичних компаній готові запропонувати гостям різноманітні тури, починаючи від гірськолижних курортів у Карпатах взимку і закінчуючи відпочинком на пляжах Балтики влітку, екскурсіями до фортець і замків Польщі, а також старовинними польськими містами, екологічним туризмом та іншими. Важливо відзначити, що відпочивати у Польщі значно дешевше, ніж в інших країнах Євросоюзу.

Створення позитивного образу країни є, перш за все, завданням держави (*Соза Відал А.К., 2019*). Польща вирішила цю проблему, створивши мережу регіональних відділень та представництв за кордоном у країнах, які є потенційно перспективними для залучення іноземних туристів. Створення такої мережі представництв допомогло вирішити проблему диспропорційного розвитку в'їзного та виїзного туризму та збільшити конкурентоспроможність туристичного продукту. Досвід Польщі є яскравим прикладом успішної реклами національного туристичного продукту. Уряд країни активно проводить маркетингові кампанії для просування свого туристичного бренду, що є взірцем для найкращих світових практик. Основну роль у рекламі та розвитку польського туристичного продукту європейська спеціалізована державна установа – Польська туристична організація, яка має представництва в 14 країнах світу, які активно взаємодіють у проведенні різноманітних туристичних заходів, моніторингу ринків країн відповідно до їх розташування, проведених рекламних інтересах та залучених партнерів до співпраці. Польська туристична організація організовує численні рекламні ініціативи, семінари, тренінги та видання рекламних матеріалів про Польщу, що просуває активний, діловий та spa-туризм, а також туристичні цінності міст і регіонів, у тому числі пам'ятки ЮНЕСКО.

Дуже ефективною для підвищення іміджу Польщі виявилася рекламна ініціатива під назвою «Залишаюся в Польщі». У рамках цієї кампанії були розповсюджені плакати зі зображенням молодого сантехніка та написом «Залишаюся в Польщі, приїздіть до нас». Це сприяло зміні стереотипів про Польщу як про країну з малокваліфікованою робочою силою. Наступний плакат містив зображення польки-медсестри з закликом вибиратися на лікування в польські санаторії. Ця рекламна ініціатива здобула значний успіх серед європейців і сприяла збільшенню кількості іноземних туристів, які обирають Польщу. Польська туристична організація розробила рекламний слоган – «Polska. Move your imagination» та систему візуальної ідентифікації Польщі – колаж з візуальних тем та іконок, пов'язаних з Польщею і її культурою. Завданням цього колажу – показати різноманіття і привабливість польської

спадщини з різних точок зору, як в сучасному стилі, так, і в старих традиціях народного мистецтва.

Для підтримку туристичного бренду уряд Польщі профінансував відновлення транспортної інфраструктури, зокрема будівництво швидкісних доріг та автомагістралей, а також реконструкцію залізничних колій. Приділялася увага відновленню історичних споруд, розвитку спортивних об'єктів, створенню науково-технічних парків та будівництву очисних споруд. Цікавим експонатом, фінансовими коштами ЄС, є адаптація до туризму – Гроти Нагоржицькі, які відображають залишки піщаної шахти, що розташована біля склозаводу. Також, варто зазначити, що у Польщі був запущений проєкт «Мені подобається Польща!», метою якого було підвищення конкурентоспроможності Польщі на азіатських ринках – Китаю, Індії та Японії. Реалізація проєкту спрямована на підвищення прибутків і витрат іноземних туристів з цих країн. Проєкт був спрямований на підвищення зацікавленості до туристичної пропозиції п’яти воєводств східної Польщі з орієнтацією на вітчизняних (в тому числі жителів Східної Польщі) і іноземних туристів (Німеччина, Україна).

З метою поляризації сільського туризму реалізується програма «Виявлення, поширення і просування передового досвіду в туризмі в сільській місцевості – продовження», метою якої є виявлення, поширення і рекомендація передового досвіду в розвитку сільського туризму в Польщі. Польська туристична організація проводить конкурс «У селі найкраще», метою якого є виявлення та просування передового досвіду туризму в сільській місцевості. Організація виступила також розробником програми щодо просування медичних послуг. Важливим маркетинговим інструментом для просування національного туристичного бренду Польщі є суть в загальноєвропейській програмі EDEN. Так, з 2007 по 2015 рік п’ять польських туристичних напрямків виграли нагороду «EDEN» від ЄС (рис. 4).

Рис. 4. Польські туристичні дестинації, які виграли нагороду «EDEN» від ЄС

Протягом останніх років за підтримку уряду Польщі були запроваджені та успішно виконані різноманітні програми для підтримки внутрішнього туризму. Серед них варто

відзначити реалізацію ініціативи «Польща: бач більше – вихідні за півці», спрямованої на стимулювання активності внутрішнього туризму.

З метою сприяння розвитку сфери ділового туризму і з використанням фінансової підтримки від держави та Польської асоціації конференцій та конгресів (SKKP) було ініційовано проект «Meet in Poland», який діє з 2027 р. Ця ініціатива передбачає створення бізнес-туристичної мережі у п'яти найбільших містах Польщі, яка об'єднала провідні MICE-компанії країни. Основною метою цього проекту є формування стійкого іміджу Польщі як привабливого бізнес-майданчика для проведення міжнародних конференцій та конгресів високого рівня. «Польські туристичні бренди» – ініціатива, яка належить Міністерству розвитку та Польській туристичній організації. Метою цього нового проекту є формування туристичних регіонів, які будуть функціонально пов'язані один з одним та цілковито відповідальні за керування розвитком та просуванням туризму на конкретних територіях. Організація умов для тісної співпраці між туристичними організаціями, органами місцевого самоврядування та учасниками туристичної галузі є ключовим аспектом даного проекту. Важливим інструментом електронного маркетингу для популяризації національного туристичного продукту є створення мобільних електронних додатків до смартфонів та планшетів (Poland.Travel, Thetripplanner, GuideWithMe, MapofPoland, Poland A GuidetoMajorCities, CastlesofPoland, SkiRaport), які одночасно є туристичними путівниками, «планувальниками подорожей» та навігаторами.

Використовуючи успішний досвід Польщі, необхідно розробити для України «Стратегії просування національного туристичного продукту за кордоном» і це стає доцільним з обов'язковим визначенням принципів створення та функціонування туристичних представництв за кордоном.

У Польщі туризм виступає каталізатором солідарності, людино-орієнтованої моделі суспільного розвитку та консолідації суспільства. Зауважимо, щоб забезпечити ефективне державне регулювання, необхідне наукове та методичне забезпечення. Розробка стратегії розвитку туристичної галузі та створення умов для її успішної реалізації є складним завданням. Для досягнення успіху та уникнення помилок слід використовувати досвід інших країн. Наприклад, міста Польщі прагнуть привернути увагу не лише історичними пам'ятками, але й сучасною архітектурою та інтерактивними музеями.

Державні органи Польщі в сфері туризму визначають і реалізують ключові напрямки державної політики, орієнтованої на розвиток туризму. Серед основних завдань можна виділити (рис. 5):

Визначення та реалізація стратегій:	• Розробка та впровадження стратегій розвитку туризму національного рівня.
Класифікація та оцінка туристичних ресурсів:	•Встановлення порядку класифікації, оцінки, використання та охорони туристичних ресурсів.
Фінансування та програми розвитку:	•Спрямування бюджетних коштів на розробку та реалізацію програм розвитку туризму.
Безпека туризму:	•Визначення основ безпеки туризму та забезпечення їх виконання.
Нормативне регулювання:	•Регулювання відносин у галузі туризму, ліцензування, стандартизація та сертифікація туристичних послуг.
Статистичний облік:	•Встановлення системи статистичного обліку і звітності в галузі туризму.
Міжнародна співпраця:	•Участь у розробці та реалізації міжнародних програм з розвитку туризму.

Рис. 5. Напрями туристичної політики Польщі (Poland.Travel, Thetripplanner, GuideWithMe, MapofPoland, Poland A GuidetoMajorCities, CastlesofPoland, SkiRaport)

Успіх туристичної галузі Польщі обумовлений не тільки вдосконаленням існуючих механізмів, але й створенням нового господарського механізму, що враховує взаємодію економічних та інституційних механізмів. Ефективність державного регулювання в туристичній галузі залежить від вивчення та впровадження різноманітних інструментів, механізмів і моделей державного управління на регіональному рівні.

Місцеві туристичні організації в Польщі відіграють важливу роль у зборі та оновленні даних про туристичні ресурси, а також у створенні та просуванні місцевих туристичних продуктів. Пріоритетними напрямками розвитку туризму в Польщі є створення привабливих туристичних продуктів на різних рівнях, включаючи місцевий, регіональний та міжрегіональний.

Для України, аналіз і використання польського досвіду в розвитку туризму може стати важливим джерелом рекомендацій для покращення власної туристичної галузі.

У Польщі існують організації та агентства, які відіграють важливу роль у розвитку туризму та захисті прав туристичних підприємств. Декілька ключових організацій та їхні функції включають:

1. Польська палата туризму. Ця організація об'єднує провідні туристичні, страхові, транспортні, готельні, торгівельні компанії, а також навчальні заклади туристичного профілю. Мета палати – лобіювання інтересів розвитку туризму та захист прав підприємців у сфері туризму.

2. Польське Агентство з розвитку туризму. Засноване у 1993 році, це агентство надає фінансові та консультаційні послуги в сфері туризму. Його завдання включає участь у створенні та реалізації проектів і програм підтримки розвитку індустрії туризму.

3. Інститут туризму. Заснований у 1972 році, цей інститут забезпечує науковий супровід розвитку туризму в Польщі. Він проводить дослідження туристичних ринків, розробляє стратегії розвитку туризму, визначає маркетингові аспекти національного туризму та оцінює економічний вплив туризму на країну.

4. Польська туристична організація. Активно співпрацюючи з іншими національними туристичними організаціями світу, ця організація приймає участь у міжнародних туристичних виставках та використовує соціальні мережі для просування туристичних пропозицій Польщі.

Польське управління туристичною галуззю також активно використовує рекламні та просувальні стратегії, щоб залучити увагу внутрішніх та зовнішніх туристів. Різноманітні заходи, такі як музичні фестивалі, лицарські турніри, свята локальної кухні та інші події, роблять країну привабливою для відвідування. Крім того, вступ до Євросоюзу сприяв розвитку туризму, забезпечивши доступність та полегшивши пересування в межах Європи.

Україна може взяти до уваги польський досвід у створенні ефективної стратегії розвитку туризму, лобіюванні інтересів галузі та використанні різноманітних заходів для привертання туристів.

Розглянемо досвід Франції. Вплив на туристичну політику Франції значною мірою визначається принципом децентралізації. Передача повноважень місцевим органам самоврядування, підтримка локальних ініціатив, розширення усіх аспектів соціального туризму та принцип всебічної співпраці між урядом, територіальними громадами та підприємцями у сфері туризму є ключовими аспектами цього впливу.

Важливо звернути увагу на підтримку соціального туризму в Україні через державну підтримку, подібну до тієї, що розглядається у Франції. Наприклад, розробка національної програми «Туризм для інвалідів», визначення відповідних нормативних актів для підтримки туристичних послуг для людей з обмеженими фізичними можливостями, затвердження національного стандарту якості туристичного продукту для сімейного відпочинку, контроль цін на певні туристичні продукти, впровадження системи відпускних чеків та підтримка системи «культурних карток», а також створення спеціальної туристичної інфраструктури для молоді тощо.

Порівнюючи з туристичною галуззю Франції, варто відзначити, що Україна, хоча й має значний туристично-рекреаційний потенціал, розвивалася без врахування своїх функціональних особливостей та без системного розуміння проблем галузі. Відсутність

цілеспрямованої та комплексної туристичної політики, відпрацьованих механізмів управління призвела до переорієнтації туризму на виїзний, руйнування системи соціального туризму та інфраструктурних компонентів галузі (*Соза Відал А.К., 2019*).

Однією з основних проблем розвитку туристичної галузі в Україні є відсутність суттєвої державної підтримки місцевих ініціатив з розвитку туризму. На основі французького досвіду можна визначити, що досягнення максимального ефекту в розвитку туризму можливе лише через співпрацю між органами виконавчої влади, місцевим самоврядуванням, громадськими та професійними організаціями та підприємницькими структурами.

У Франції відповідальність щодо регулювання сфери туризму належить Міністерству транспорту та суспільних робіт. В структурі цього відомства функціонують Державний секретаріат з питань туризму та Управління туризму. Ці органи відповідають за управління та регулювання галузі, включаючи інвестиції та міжнародні відносини в туризмі. Крім того, існують різні органи, які беруть участь у керівництві туризмом з правом консультативного голосу, такі як Рада з туризму при Міністерстві транспорту та суспільних робіт, Французьке агентство туристичного інжинірингу, Національна наглядацька рада з туризму (маркетингові дослідження й статистика в туризмі), Національне агентство з питань відпускних подорожей (соціальний туризм), Національний комітет з процвітання Франції (питання екології й озеленення міст) (*Домбровська С.М., Білотіл О.М., Помаза-Пономаренко А.Л., 2016*).

На регіональному рівні представники центральної виконавчої влади вирішують питання розвитку туристичної галузі і підпорядковані префектам. Їхні дії спрямовані на координацію регіональних ініціатив, оскільки повноваження місцевої влади в галузі туризму є дуже вагомими. Французька асоціація «Maison de la France» («Будинки у Франції»), створена в 1987 році через партнерство між місцевими адміністраціями, суб'єктам туристичної діяльності, закладам готельного й ресторанного господарства та адміністраціями об'єктів екскурсійного показу, відіграє ключову роль у просуванні образу Франції як туристичного центру на міжнародному ринку (*Домбровська С.М., Білотіл О.М., Помаза-Пономаренко А.Л., 2016*).

З урахуванням досвіду Франції, туристична галузь України стикається з численними проблемами, які потребують вдосконалення системи та механізмів державного управління. Для поліпшення ситуації необхідно вдосконалити механізми регулювання господарської діяльності, враховуючи здобутий досвід Франції. Також, необхідно формувати нові соціально-економічні підходи до стратегії розвитку національного туристичного комплексу та системи управління туристичними процесами на державному та регіональному рівнях. Один із шляхів вирішення цих проблем – розробка та прийняття комплексної державної Програми розвитку

соціального туризму в Україні, включаючи законодавчі акти, такі як «Про соціальний туризм», «Про молодіжний та дитячий туризм», а також розробку Концепції розвитку спеціалізованої туристичної інфраструктури (*Помаза-Пономаренко А.Л. 2022*).

Щодо країни, яка межує з Україною через сусідню Польщу – Чехії, економіка якої ґрунтується на принципах відкритого ринку. Уряд Чехії активно сприяє залученню інвестицій у свою економіку, в тому числі й в сферу туризму. Чеська Республіка поступово зміцнює свої позиції на світовому туристичному ринку, стаючи популярним європейським напрямком з розвиненим туризмом.

Розвитком туризму в Чехії керує державна організація CzechTourism *(CzechTourism*), яка просуває Чеську Республіку як привабливу туристичну дестинацію.

Для кожного регіону Чехії розроблено власну унікальну програму розвитку туризму, яка враховує місцеві особливості, але має загальні засади і стратегічні цілі. Цей досвід успішного формування та розвитку туристичного потенціалу може бути корисним для України. Особлива увага приділяється екологічним, соціокультурним і економічним аспектам туристичної діяльності Чехії. З метою підвищення привабливості Чеської Республіки, відповідно до Концепції державної політики у сфері туризму, робиться акцент на рис. 6:

Рис. 6. Основні акценти концепції державної політики (*Помаза-Пономаренко А.Л. 2022*)

Туристична політика Чехії передбачає організацію туристичних ярмарків і виставок, проведення семінарів, презентацій та рекламних кампаній, а також встановлення маркетингових партнерських відносин з регіонами. Всі ці інструменти використовуються для

просування національних та регіональних туристичних продуктів. Реалізація принципів державної туристичної політики в області маркетингу зовнішніх послуг визначає успіх у збільшенні в'їзних туристичних потоків та покращенні якості в'їзного туризму. З метою зростання туристичних потоків в країну, концепція державної туристичної політики передбачає підвищення якості послуг через покращення кваліфікації працівників, використання сучасних інформаційних систем, а також поліпшення обслуговування тощо.

Проведення засідань Ради стратегії розглядається не рідше одного разу на рік, а збори скликаються директором за умови наявності абсолютної більшості членів. Позачергові збори Ради стратегії можуть бути скликані в разі термінової необхідності за запитом абсолютної більшості членів Ради або директора CzechTourism. Впровадження державної туристичної політики країни відбувається відповідно до принципів «Концепції державної політики в галузі туризму в Чеській Республіці», яка визначає комплекс заходів для досягнення основних цілей політики в галузі туризму. Основний акцент робиться на підвищенні конкурентоспроможності та економічної вигоди від туризму, зменшенні рівня безробіття, розвитку регіонів, малих та середніх підприємств, охороні навколишнього середовища. Першочергові завдання, визначені концепцією:

1) забезпечення конкурентоздатності національних та регіональних продуктів у сфері туризму;

2) розвиток та удосконалення інфраструктури для надання туристичних послуг;

3) використання маркетингових стратегій у сфері туризму та розвиток людських ресурсів;

4) створення організаційної структури для управління туризмом.

Роль CzechTourism у втіленні державної туристичної політики полягає у визначенні всіх учасників, залучених до процесу сталого розвитку туризму, спілкуванні та співпраці з ними, розробці проектів та вирішенні проблем у сфері туризму Чехії.

Ще однією ключовою метою державної туристичної політики Чехії є реалізація інтересів країни за кордоном в контексті в’їзного туризму та підтримка внутрішнього туризму. Ця мета включає два основних напрями: створення пропозиції та формування попиту. Аналітичні дослідження, проведені Czech Tourism, спрямовані на вивчення тенденцій розвитку міжнародних туристичних потоків, оцінку ефективності використання наявних ресурсів та аналіз попиту та пропозиції.

Для популяризації країни в інтеренет-мережі CzechTourism адмініструє кілька спеціалізованих веб-порталів. Серед найважливіших – Kudy z nudy, Czechtourism.com,

Czechtourism.cz, The Czech Republic – a Land of Stories та the CzechMobil, орієнтовані на активний туризм.

Розглядаючи просування Чехії, Чеська агенція туризму розпочала маркетингову кампанію «Чехія – країна історій», орієнтовану на розкриття унікальних культурних аспектів, гастрономії, традицій та звичаїв країни. Національна туристична стратегія формуються як «Чехія – ключовий пункт у серці Європи». Основна мета цієї стратегії – підвищення конкурентоспроможності туристичного сектору на національному та регіональному рівнях, а також підтримка економічного зростання.

Одна з ключових ініціатив, а саме програма «Туризм для всіх» орієнтована на розробку нових продуктів для внутрішнього туристичного сектору. Ці продукти включали в себе не лише нові розваги, такі як доступ для інвалідних візків, ігрові кімнати для дітей, ігрові майданчики та пересувні басейни, але й проведення маркетингових заходів для їх рекламування та впровадження. У 2011 році була оголошена ще одна програма – «Туризм, доступний для всіх», що спрямована на реконструкцію та будівництво зон відпочинку, санвузлів для туристів, велосипедистів і осіб із обмеженими можливостями.

У2019–2021 рр. діяла програма просування Чехії за допомогою кампанії «Як Чехія». Основною комунікаційною темою стануть міста, розглядувані як ворота до регіонів, на які спрямована маркетингова діяльність штабу та закордонних офісів.

Проаналізувавши розвиток туризму в регіонах та вивчивши основні принципи формування стратегії регіональної політики Чеської Республіки (*Michael Porter, 2011*), вважаємо за доцільне для України розробити концепцію туристичного розвитку. Основні напрями цієї концепції включають:

– створення єдиного туристичного бренду країни із унікальними регіональними особливостями.

– концепція розвитку підприємництва.

– фінансова стратегія, яка включає розробку бізнес-планів для розвитку туристичних територій та визначення джерел фінансування.

– управлінська концепція, що охоплює розробку стратегії управління та заходів для підготовки управлінських кадрів.

– маркетингова концепція, включаючи розробку та впровадження маркетингової стратегії та комплекс дій для формування позитивного іміджу регіону.

З досвіду Чеської Республіки виходить, що ключовим позитивним елементом у розробці стратегії розвитку туристичних регіонів є наявність добре визначеної організаційної структури. Серед соціально-економічних факторів, що сприяють розвитку регіонального

туризму в Чехії, важливе значення приділяється таким чинникам, як підвищення рівня освіти, культурний рівень та естетичні потреби населення.

В Угорщині відбулася повна реорганізація Управління з туризму, і зараз цей сектор економіки перейшов під управління Національного агентства з туризму при Міністерстві національного розвитку. Однією з пріоритетних завдань цієї структури є координація маркетингу туризму на національному рівні. Це включає розвиток системи брендингу туризму в Угорщині, а також вітчизняної та міжнародної маркетингової та комунікаційної діяльності, а також розвиток та комунікацію брендового туризму країни. Окрім цього, ця структура працює над розвитком туристичного іміджу та загального іміджу Угорщини. В Угорщині також був розроблений план Сечені, який виділив 100 млн євро на розвиток туризму та реалізацію заходів з поліпшення туристичної інфраструктури.

З метою підвищення туристичної привабливості та розвитку в Угорщині, розпочато імплементацію програми туристичного брендингу. Основне завдання полягає в розробці та створенні оновленого туристичного бренду для країни з метою зробити Угорщину бажаним та привабливим напрямком для як іноземних, так і місцевих туристів. Основним прагненням в міжнародному контексті є ефективне позиціювання Угорщини та визначення міжнародного бренду країни, зокрема Будапешти, відповідно до їхнього потенціалу в Європі. Структура брендингу підтримує розробку відповідних пропозицій, орієнтованих на різні сегменти туристичного ринку, та реалізацію спеціалізованих маркетингових кампаній на кожному рівні. Ключовими компонентами системи бренду від верхнього до нижнього рівня є: бренд Угорщини, бренд Будапешта, пріоритетні галузі розвитку туризму, туристичні продукти, окремі постачальники туристичних послуг, пам’ятки і елементи інфраструктури.

У 2018 році Національне агентство з туризму Угорщини запустило свою ініціативу з комплексного просування у Будапешті, охоплюючи різні мовленнєві платформи, такі як онлайн, друковані ЗМІ і телебачення, на ключових мовленнєвих ринках. Основна ціль кампанії полягала в визначенні атракційних місць та видів діяльності столиці для відвідувачів, які є відкритими, мотивованими і бажають отримати якісний туристичний досвід. Перероблений імідж туризму в Будапешті базується на концепції "Спеції Європи" в Будапешті, що виражає ідею, що гості, що відвідують місто, знайдуть все, що характерне для типової європейської столиці: історична спадщина, різноманітні культурні пропозиції, висококласна гастрономія і мода. У межах кампанії «Spice of Europe» було створено новий туристичний логотип, оновлений веб-сайт та креативний контент, а також новий іміджевий фільм, що ілюструє Будапешт і метафоричну «пряність» столиці.

Щодо Словаччини, найважливішою державною структурою в туристичній галузі є Департамент туризму, що підпорядковується Міністерству транспорту та будівництва. Основні завдання включають розробку, впровадження та оцінку стратегічних та концептуальних матеріалів для розвитку туризму в Словацькій Республіці, а також висунення пропозицій стосовно загальнообов'язкового законодавства, пов'язаного з туризмом.

У межах ініціативи «European Quartet – One Melody» здійснювалося спільне просування туристичного продукту, яке відбувалося в рамках співпраці між країнами Вишеградської четвірки для виведення на світовий ринок. Це включало ініціативу національних туристичних інститутів Словаччини, Польщі, Чехії та Угорщини.

Для популяризації туристичного бренду Словаччини в інтернет-мережі було розроблено новий Інтернет-портал – http://www.slovakia.travel (*Інтернет-порталу*). Це офіційний інформаційний портал про туризм у Словаччині з представленням важливої та загальної інформації про туризм, культурні спільноти, історичні та природні об'єкти (в основному ЮНЕСКО), актуальних туристичних продуктах у Словаччині, а також туристичні карти, фотографії, віртуальні тури.

У Словаччині було впроваджено Національний проєкт NUTIS (Національна єдина туристична інформаційна система), що призвів до створення порталу інтернет-туризму slovakia.travel. Керівництво системою контенту здійснювалося AiCES, яка включала 10 обраних туристичних інформаційних центрів, охоплюючи 8 регіонів Словаччини. З метою наслідування позитивного досвіду Нідерландів, Данії та Німеччини, які відзначалися значною кількістю велосипедистів на вулицях міст, Словаччина розробила та реалізувала стратегію для впровадження конкретних заходів, спрямованих на популяризацію велосипеда як транспортного засобу і засобу відпочинку.

Говорячи про їжу та диференціацію країн, вивчення тенденцій туризму є неминучим оскільки переважна більшість досліджень, пов'язаних з їжею та брендингом країни, пов'язані з сферою туризму (*Berg, P., & Sevón, G., 2014).* Проте цей зв'язок між їжею, культурою та туризмом, був визнаний лише дослідниками, урядами та промисловістю з середини 1990-х років. Щоб залучити більше туристів, багато місць вирішили встановити міцніші стосунки між їжею та маркетингом, з метою одночасного зміцнення свого туризму. Багато дослідників відзначають успіх будь-якої туристичної стратегії, яка також покладається на їжу в цьому місці та їх стійку конкурентоспроможність.

Туризм намагається популяризувати та розмежовувати кожну країну та місто з певними аспектами зробити їх впізнаваними та привабливими для туристів. Брендування міста чи країни через його культуру харчування, претендує на те, щоб не тільки залучити більше

туристів, але й створити такий імідж, що описує та приваблює людей, які там живуть. На рис. 7 представлено брендування міст Італії на основі гастрономічних особливостей.

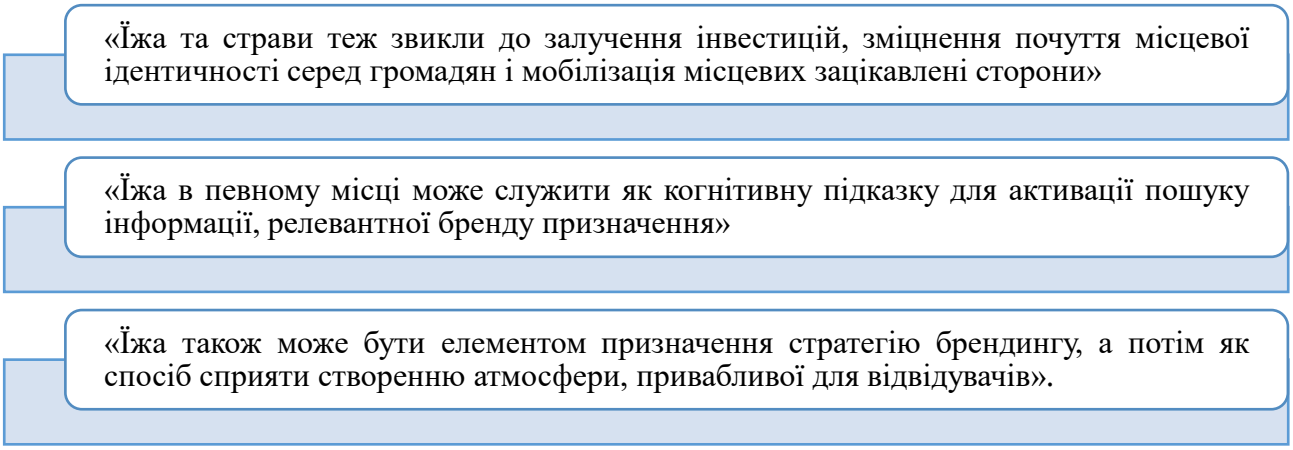


Рис. 7. Брендування міст Італії на основі гастрономічних особливостей

Існують інші стратегії, які міста чи країни активно використовують для брендування своєї ідентичності щодо їжі. Усілякі події, такі як фестивалі, ярмарки та виставки, пов'язані з харчові або архітектурні чи просторові трансформації міста, такі як створення продовольчих ринків або трансформація фуд-холів.

Спільним для всіх цих видів діяльності є промоція країни через їжу бренд і імідж. Цей зв'язок незаперечний, коли прямо чи опосередковано цей образ країни створюється за допомогою їжі та гастрономії як такої чи як частини культури.

Зрозуміло, що культура харчування підвищилася завдяки співпраці і зросла видимість журналістів і блогерів в Інтернеті. Рекомендується всім акторам, зацікавлені сторони та організації, які беруть участь у створенні іміджу місця чи призначення, створюють узгоджені повідомлення для забезпечення успішного маркетингу. Спілкування має бути зміцнення між усіма частинами, пов'язаними з використанням їжі для просування цих місць.

Цей розділ дослідження робить висновок про важливість і чіткий взаємозв'язок між різними аспектами країни у створенні її бренду, іміджу та ідентичності.

Було підкреслено культуру та їжу, а в наступному розділі висвітлено побудову Італії як бренду, її культуру, сектор харчування та гастрономію. Для цього важливо також підкреслити контекст і середовище країни досліджується брендинг: італійський бренд на харчовій сцені України.

Стратегія присвячена застосуванню громади і місцеві інтервенції, цілями яких є впровадження благополуччя та доступ до основних послуг у так званих внутрішніх районах, а саме районах, розташованих справедливо віддалені від міських центрів і міських вузлів.

Одне з можливих «рішень периферійності», яке часто виникає з політичні документи, створені в рамках SNAI, є переходом до більш орієнтованої на туризм економіки. Потенційний

успіх розвитку туризму у периферійних районах часто сприймається як належне на основі їх незайманої території капіталу, незалежно від їх фактичних структурних можливостей. Цей погляд створює коротке замикання між просторово-сліпими припущеннями в рамках місцевої політики підхід. З теоретичної точки зору розвиток туризму вивчає регіональну політику розвитку, аналізує розвиток туризму в периферійних районах, а туризм розглядається лише як один із можливих елементів більш структурована політика розвитку, спрямована на сприяння основним послугам для населення

Іспанія завжди була дуже відомим туристичним напрямком. Упродовж кількох останніх років туристична галузь Іспанії демонструє високі темпи розвитку, тому сьогодні вона безумовно виступає потужним інструментом в економічному секторі країни. Згідно з даними Національного інституту статистики, в 2018 році Іспанію відвідало 82,77 млн. іноземних туристів і цю цифру вже можна вважати новим туристичним рекордом. У списку найвідвідуваніших країн світу вона розташувалась на другій сходинці саме завдяки таким показникам прибутків. Нині серед найпопулярніших дестинацій її головним конкурентом залишається тільки Франція. За кількістю надходжень від туризму до пандемії, Іспанія посіла третє місце.

Туристи обирають Іспанію як популярний туристичний напрямок, тому що комфорт, хороший сервіс, гостинність і турбота в готелях є основними факторами при виборі країни відпочинку. Туризм вимагає від уряду інвестування додаткових коштів у розвиток міст, створення парків та дитячих майданчиків. Оскільки Іспанія – це не тільки море, сонце та пісок, для збільшення кількості туристів необхідно розробляти та пропагувати нові туристичні проекти, спрямовані на просування продукту країни на міжнародному туристичному ринку. У цій ситуації реалізація та розвиток різноманітних програм на національному рівні сприятиме розвитку туризму та сприятиме відновленню та збереженню природи. Туризм сприяє збереженню миру та злагоди між країнами. Країни отримують дохід не лише від туризму, а й від міжнародних перевезень. І це становить значну частину додаткових коштів, які генерує уряд.

Зростання туризму в Португалії дозволило збільшити економіку в останнє десятиліття більше, ніж будь-яка інша економічна діяльність. Позитивні результати за багатьма показниками, такими як внесок у ВВП, експорт і доходи, свідчать про те, що його вважали локомотивом економіки, який дав результати в усіх регіонах країни. Також цим результатам сприяли різні стратегії, які уряд постійно визначав протягом останніх двох десятиліть. Ця стаття починається з короткого огляду літератури та представляє описовий аналіз основних довгострокових інструментів, які характеризують португальську стратегію туризму,

показуючи важливу роль, яку планування може мати в управлінні впливом, що виникає в результаті здійснення цієї діяльності. Також представлені результати основних показників (опубліковані кількома різними джерелами). Результати показують, що все ще є кілька проблем, які потребують вирішення, тому розкриваються основні виклики для розвитку туризму в Португалії.

Туристична стратегія Греції спрямована на просування країни як всесвітньо відомого та привабливого напрямку для відпочинку, який пропонує унікальні та оригінальні туристичні враження. Розвиток туризму є ключовим аспектом державної політики стосовно національного розвитку, інновацій та відкритості. Зрозуміло, що однією з викликів у розвитку туризму в Греції є зменшення масштабів подорожей через пандемію COVID-19. У 2019 році ВВП країни знизився на 8,2%. Сфера туризму складає близько п'ятої частини грецької економіки та ринку праці, і після невдалого для цього сектору минулого року країна не могла дозволити собі ще одного "втраченого літа". Тому, влітку 2021 року Греція однією з перших країн в Європі почала приймати українських туристів для відпочинку. Основними пріоритетами національної туристичної політики є підвищення конкурентоспроможності, якості, оригінальності та стійкості туристичного продукту, а також збільшення інвестицій у високоякісне розміщення та інші туристичні проекти з низьким впливом на навколишнє середовище. При цьому враховуються цілі сталого розвитку ООН.

Загалом виявляється, що розвиток туризму в Греції має полярний характер центром якого є острівні комплекси, де розташовано майже 52% готельних місць трьох регіонів (Кріт, Додеканес). Ці регіони мають певну закономірність розвитку, як модель масового туризму, в якій післявоєнний розвиток робили ставку на індустрію туризму в країні. Однак є регіони, які мають невикористані туристичні ресурси, які можуть бути використані в контексті ендогенного інтегрованого розвитку туризму. Крім того, встановлено, що основна причина створення туристичної нерівності залишається структурною проблемою грецького туризму та особливо закон, який часом заохочував незбалансовану концентрацію туристів діяльність, а також неправильне планування розвитку післявоєнного періоду, що призвело до надмірна концентрація туристичної пропозиції в окремих районах, їх безрозсудний заряд природного навколишнього середовища, насичення і занепад у деяких районах. Це призвело до створення а протиріччя в розвитку туризму, що призводить до низької ефективності і, як наслідок, низької конкурентоспроможність у туризмі. Протиріччя ґрунтується на спостереженні, що збільшення загального розміру туристичного обміну не пов'язане з збільшенням середніх туристичних витрат на одного туриста у дефльованих цінах, а навпаки, спостерігається тенденція до зниження. Це ознака низького рівня доходу туристів, що сильно впливає на якість

і валютні можливості. З іншого боку, він не враховується і не оцінюється внеском внутрішнього туризму, який є важливим параметром збалансованого розвитку туризму країни.

Поширені уявлення про соціально-економічну роль туризму в економіці Монако є перебільшеними та не відповідають дійсності. Туризм є одним із основних секторів економіки князівства в Монако, яке загалом має диверсифіковану економіку з акцентом на розвиток торгівлі, високих технологій, наукових досліджень і розробок. Туристичний ринок Монако характеризується чергуванням періодів різкого спаду і зростання туристичних доходів, що відображає його залежність від соціально-економічних факторів та інших чинників, які мають місце у світі і насамперед у Європі. Загальна тенденція розвитку внутрішнього туризму в Монако за останній період демонструє певну стагнацію, що в основному пов'язано з недавньою світовою кризою. Перспективи розвитку туристичного ринку Монако будуть визначатися не тільки реалізацією стратегії відновлення високих темпів попередніх років, а й зовнішніми факторами. Тому уряд країни безумовно хоче розвивати в країні міжнародний туризм і стежити за тим, щоб інтерес іноземних туристів до Монако не зникав. Але це не означає, що економіка країни значною мірою залежить від туризму (Michael Porter, 2011).

Туристична діяльність організована на трьох рівнях: національному, регіональному та місцевому. На національному рівні розроблено загальну туристичну політику, розроблено короткострокову, середньострокову та довгострокову стратегію, сертифіковано туристичні об’єкти, розроблено програму просування туристичного бренду Болгарії на міжнародному рівні. . Країна розроблена і реалізована. Відповідно до законодавства країни, регіональна влада має розробляти регіональні програми розвитку туризму та контролювати їх виконання місцевими установами. Місцеве управління туризмом в Болгарії є відповідальністю місцевих органів влади, мерів міст і селищ. Вони беруть участь у розробці та реалізації програм розвитку туризму та маркетингу у своїх регіонах, сертифікації закладів гостинності нижчого класу (готелів 2 зірки, готелів, ресторанів, пансіонатів), моніторингу якості туристичних послуг Працюють, створюють підтримувати мережу туристично-інформаційних центрів (ТІЦ) тощо. Крім того, в країні є мережа місцевих організацій, які також займаються управлінською та маркетинговою діяльністю для залучення туристів до місць призначення. Однією з ознак децентралізації управління туризмом в Болгарії є створення та просування напрямків, що визначено державною програмою розвитку галузі (Ivanov S.,2014).

Створення міжнародного туристичного образу країни стає надзвичайно важливим у сучасних умовах глобалізації та посиленої конкуренції між країнами. Україні необхідно розвивати міжнародний туристичний бренд, який визначатиме привабливість її туристичного ринку. Ключові конкурентні переваги, що визначають привабливість України для

європейських споживачів, включають наявність об'єктів культурно-історичної спадщини, вигідне розташування, рекреаційний потенціал, розвинений соціокультурний стан країни та економічна привабливість туристичних подорожей. Елементи міжнародного туристичного бренду України повинні включати гостинність, щирість, щедрість, толерантність, недоторкану природу, архітектурні пам'ятки та унікальні релігійні святині. Основою бренду повинно бути розуміння, що Україна – це перехрестя цивілізацій, релігій і культур, кордон Європи та Азії з унікальною та стародавньою історією. Для втілення цієї моделі ідентичності міжнародного туристичного бренду України необхідно розробити програми впровадження стратегії просування бренду на міжнародному рівні. Для створення та управління міжнародним брендом країни слід залучити державні та приватні організації на етапі розроблення нормативно-правових засад для формування стійкого міжнародного бренду та розвитку державно-приватного партнерства у сфері розроблення та реалізації стратегії просування бренду України.

Отже, дослідження стратегій формування туристичного брендингу в окремих країнах Центрально-Східної Європи свідчить про їхню відмінну активність. Це свідчить про збільшення рівня визнання країн за кордоном як привабливого місця для туристів та наявність конкурентоздатних туристичних продуктів високої якості. Зміни були досягнуті завдяки комплексу ефективних заходів з просування національного туристичного продукту за активної участі державних структур, впровадженню проектів для розвитку різних видів туризму, інвестиціям у туристичну інфраструктуру з боку держави та ЄС, а також участі в загальноєвропейських туристичних заходах та інше.

Провівши аналіз досвіду державного управління у формуванні туристичного потенціалу в Польщі, Франції, Угорщині, Словаччині, Чехії, Італії, Іспанії, Португалії, Греції, Монако, Болгарії можна зробити наступні висновки:

1. Загальним напрямком у Європейській практиці є підтримка розвитку туристичної галузі та формування туристичного потенціалу країни. Це досягається створенням ефективних державно-управлінських інституцій, які взяли б на себе компетенції у сфері туризму, наданням значної інвестиційної підтримки для формування туристичного потенціалу та сприянням розвитку ключових туристичних регіонів країни.

2. У цих країнах приділяється велика увага формуванню позитивного туристичного іміджу країни на міжнародному рівні.

3. Дослідження Європейських країн свідчать, що Україна має унікальні природні та історико-культурні ресурси, а також потенціал стати важливим туристичним напрямком. Для досягнення цієї мети необхідно використовувати ефективне державне управління, що

сприятиме процесу формування туристичного потенціалу як інструмента консолідації суспільства та створенню сприятливих умов для розвитку туристичної галузі, наслідуючи приклад відомих туристичних країн.

4. Основними обмежуючими факторами формування та реалізації туристичного потенціалу України є такі аспекти:

неефективне використання туристичних ресурсів;

недостатнє фінансування зі сторони держави;

неузгодженість цін і якості;

нестача кваліфікованих кадрів;

неадекватний стан туристичної інфраструктури.

Ці та інші чинники, що обмежують розвиток туристичної галузі в Україні, можна подолати за допомогою раціонального державного управління та ефективних заходів, взятих за прикладом успішних країн Євросоюзу. Також на нашу думку, при формуванні туристичної політики України варто приділити значну увагу туристичному бренду спираючись на позитивний досвід Польщі, Франції, Угорщині, Словаччині, Чехії, Італії, Іспанії, Португалії, Греції, Монако, Болгарії, що дозволить підвищити рівень своєї туристичної привабливості. Для України характерним є відсутність чітко виокремленого туристичного бренду та іміджу, сильний територіальний дисбаланс, залежність від окремих видів туризму, неадекватною розвиненістю внутрішньої інфраструктури, недостатньою активністю держави у впровадженні програм підтримки туризму та нестачею фінансування. Таким чином, для України є необхідним перегляд основних принципів та методів політики туристичного брендингу. Наше дослідження підтверджує важливість проведення та підтримки іміджевої рекламної кампанії для країни на державному рівні, оскільки приватний туристичний бізнес має інтерес лише до просування власного туристичного продукту.

Висновок. Особливості формування туристичної політики в країнах Європейського Союзу є результатом складного взаємодії різних чинників, які включають культурні, економічні, соціальні та політичні аспекти. У країнах ЄС туризм є важливим галуззю, яка сприяє економічному зростанню, збагачує культурний обмін та сприяє взаєморозумінню між народами. Перш за все, варто зазначити, що Європейський Союз сприяє координації туристичної політики між своїми членами. Це дозволяє створювати спільні стандарти щодо безпеки туристів, розвитку інфраструктури та просування туристичних маршрутів. Крім того, ЄС забезпечує фінансову підтримку для проектів, спрямованих на розвиток туризму в різних регіонах.

Важливим аспектом є збалансоване управління туризмом з метою збереження природних та культурних ресурсів. Багато країн ЄС активно розвивають сталі туристичні практики, спрямовані на збереження навколишнього середовища та місцевої культури, забороняючи або обмежуючи деякі види туризму, які можуть шкодити природі або спотворювати місцевий спосіб життя. Також важливим аспектом є розвиток інноваційних технологій у сфері туризму. Це включає в себе впровадження цифрових технологій, таких як мобільні додатки, віртуальна реальність та штучний інтелект, що допомагають покращити якість обслуговування туристів та забезпечити їм більш індивідуалізований досвід подорожей.

Загалом, формування туристичної політики в країнах Європейського Союзу відбувається на перехресті інтересів різних зацікавлених сторін, враховуючи потреби економіки, культури, природи та суспільства в цілому. Використання інноваційних підходів, співпраця між країнами та збалансоване управління – ключові елементи для успішного розвитку туризму в регіоні.

Охарактеризовано основні міжнародні моделі реалізації туристичної політики, які є важливим інструментом для країн, які прагнуть ефективно розвивати свій туристичний сектор. Вони базуються на співпраці та обміні досвідом між країнами для досягнення спільних цілей. Спільні стандарти та стратегії, прийняті на міжнародному рівні, можуть сприяти сталому розвитку туризму та забезпечити гармонізацію підходів між різними країнами. Моделі також дозволяють країнам взяти найкращі практики одна від одної, сприяючи ефективній реалізації та інноваціям у туристичному галузі.

Використання досвіду країн Європейського Союзу є ключовим елементом формування туристичної політики України. Спостереження за позитивними аспектами економічного та культурного впливу туризму в ЄС може служити основою для впровадження ефективних стратегій та практик у національному туристичному секторі України. Орієнтація на принципи сталого розвитку, екологічної відповідальності та збереження культурної спадщини, взята з досвіду країн ЄС (Польщі, Чехії, Франції, Угорщини, Франції, Словаччини, Іспанії, Греції, Монако та Болгарії), може сприяти створенню в Україні більш збалансованого та високоякісного туристичного середовища. Застосування кращих практик у сфері туризму, таких як ефективний маркетинг, розвиток туристичної інфраструктури та партнерства в сфері туризму, може сприяти привертанню більшого туристичного потоку та збільшенню економічних переваг та можливостей для України.

References:

Австрійський національний туристичний офіс. URL: https://b2b.austria. info/uk/about-us/austrian-national-tourist-office. (дата звернення: 12.02.2024).

Бойко М., Гопкало Л., (2005). Засади формування пріоритетних напрямів туристичної політики України. *Регіональна економіка*. №1. С.222 – 229.

Герасименко В.Г. (2008). Управління національним туризмом у контексті міжнародного досвіду. *Вісник ДІТБ. Серія: Економіка, організація і управління підприємствами (в туристичній сфері)*. №12. С.19 – 24.

Домбровська С. М., Білотіл О. М., Помаза-Пономаренко А. Л., (2016) Державне регулювання туристичної галузі України [Монографія]. Харків: НУЦЗУ. 196 с., с. 125.

Ключник Р.М., (2020). Культурно-історичний туризм: потенціал та його реалізація. Сучасний стан та перспективи розвитку туристичної галузі: ІІІ Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених: тези доповідей, Дніпро, 26 березня 2020 р. Дніпро: Університет імені Альфреда Нобеля. С. 104 – 106.

Мальська М. П., (2015). Основи європейської інтеграції : підручник. / М. П. Мальська, Н. В. Антонюк. К. : «Центр учбової літератури». 320 с.

Матвієнко Н., Матвієнко В., (2018). Чинники розвитку туризму в Хорватії. *Вісник Київського національного університету імені Тараса Шевченка*. Серія «Географія». Вип. 3 (72). С. 81 – 88.

Національне туристичне управління Чеської Республіки. URL: http://www.czechtourism.cz/informace-oczechtourism/statut/. (дата звернення: 02.02.2024).

Офіційна сторінка Хорватської національної туристичної ради (CNTB). URL: https://www.htz.hr/en-GB/press/press-releases/tourist-nights-2022-nearly-many-2019 (дата звернення: 12.02.2024).

Офіційний сайт «CzechTourism». URL: https://www.czechtourism.com. (дата звернення: 20.11.2023).

Офіційний сайт Інтернет-порталу. URL: http://www.slovakia.travel. (дата звернення: 20.11.2023).

Помаза-Пономаренко А.Л., (2022). Розвиток туризму в Україні у воєнний та післявоєнний періоди. *Вчені записки ТНУ імені В.І. Вернадського. Серія : Публічне управління та адміністрування.* Том 33 (72). № 5. DOI: https://doi.org/10.32782/TNU-2663-6468/2022.5/02

Соза Відал А.К. Міжнародний імідж Франції: культурний аспект. Освіта і наука у мінливому світі: проблеми та перспективи розвитку. Матеріали Міжнародної наукової конференції, 29 – 30 березня 2019 р., м. Дніпро. Ч. І. / наук. ред. О.Ю. Висоцький. Дніпро: Охотнік, 2019. С. 356 – 357.

Berg, P., & Sevón, G., (2014). Food-branding places-A sensory experience. Place Branding and Public Diplomacy, Vol. 00, No. 0, pp. 1-16.

Czech Republic saw record number of tourists in 2018. Available at: https://kafkadesk.org/2019/02/10/czech-republic-saw-record-number-of-tourists-in-2018/. (дата звернення: 02.02.2024).

Ivanov S., (2014). Managing tourism in Bulgaria: Between “Mission impossible” and New Hope / S. Ivanov, M. Dimitrova // European Tourism Planning and Organisation Systems / C. Costa, E. Panyik, D. Buhalis. Exeter : Short Run Press Ltd. P. 87 – 106.

Michael Porter, (2011). MONACO’S TOURISM CLUSTER. Microeconomics of Competitiveness. Final Paper. URl: http://www.isc.hbs.edu/pdf/Student_Projects/Monaco_Tourism_2011.pdf.

Robinson Peter, Lück Michael, Smith Stephen L. J., Lackey Michael. Tourism. CABI, 2013. 525 p.

Tüsiad (2012). Sürdürülebilir Turizm/ Sustainable Tourism. Rapor, Eylül. URL: https://tusiad.org/tr/yayinlar/raporlar/item/6030-surdurulebilir-turizm. Accessed: 12.02.20243.

DOI 10.5281/zenodo.10820296
UDC 378.015.3:005.584.1

CHAPTER 3.

IMPROVING THE MANAGEMENT OF THE EDUCATIONAL ACTIVITIES OF THE INSTITUTION OF HIGHER EDUCATION BY MEANS OF MONITORING

Nataliia BORYSENKO,
Doctor of Philosophy (Pedagogy), Associate Professor, Vice-rector for Educational Work,
H. S. Skovoroda Kharkiv National Pedagogical University (Kharkiv, Ukraine)
bna0301@gmail.com
https://orcid.org/0000-0002-0532-3867

Olena GRECHANYK,
Candidate of Pedagogical Sciences, Associate Professor,
Head of the Department of Scientific Foundations of Management,
H. S. Skovoroda Kharkiv National Pedagogical University (Kharkiv, Ukraine)
grechaniklena@ukr.net
https://orcid.org/0000-0002-4671-0724

Abstract. The monograph highlights the problem of improving the management of educational activities in a higher education institution (HEI) by means of monitoring, in particular, the theoretical aspects of monitoring the educational activity of HEI are considered, the peculiarities of education in higher education are characterized, the criteria and indicators of the quality of education and its management, the stages of educational activity monitoring are revealed. The practical section of the monograph analyzes the monitoring of educational activities as a management problem. An assessment of the readiness of scientific-pedagogical and pedagogical workers of higher education institutions to monitor educational activities was carried out. A qualitative model for assessing the state of monitoring has been developed, and the level of the state of monitoring of educational activities in an educational institution has been determined. On a diagnostic basis, a complex target program (CTP) for improving the monitoring of educational activities in higher education has been drawn up, which is designed for 1.5 years and includes 4 stages. CTP examination was carried out. Methodological recommendations on the implementation of a complex and targeted program in the practice of work of higher education institutions have been provided. The

implementation of the CTP involves the creation of appropriate conditions in the educational institution: organizational and pedagogical, moral and psychological, material and technical, sanitary and hygienic, etc.

Key words: educational activity, monitoring, management, institution of higher education, qualitative model, quality of educational activity.

УДОСКОНАЛЕННЯ УПРАВЛІННЯ ВИХОВНОЮ ДІЯЛЬНІСТЮ ЗАКЛАДУ ВИЩОЇ ОСВІТИ ЗАСОБАМИ МОНІТОРИНГУ

Анотація. У монографії висвітлено проблему вдосконалення управління виховною діяльністю в закладі вищої освіти (ЗВО) засобами моніторингу, зокрема, розглянуто теоретичні аспекти моніторингу виховної діяльності ЗВО, схарактеризовано особливості виховання у вищій школі, розкрито критерії та показники якості виховання й управління ним, етапи моніторингу виховної діяльності. У практичному розділі монографії проаналізовано моніторинг виховної діяльності як управлінську проблему. Здійснено оцінку готовності науково-педагогічних і педагогічних працівників ЗВО до проведення моніторингу виховної діяльності. Розроблено кваліметричну модель оцінки стану моніторингу, визначено рівень стану моніторингу виховної діяльності в закладі освіти. На діагностичній основі складено комплексно-цільову програму (КЦП) з удосконалення моніторингу виховної діяльності у виші, яка розрахована на 1,5 роки й містить 4 етапи. Проведено експертизу КЦП. Надано методичні рекомендації з упровадження комплексно-цільової програми в практику роботи ЗВО. Реалізація КЦП передбачає створення в закладі освіти відповідних умов: організаційно-педагогічних, морально-психологічних, матеріально-технічних, санітарно-гігієнічних тощо.

Ключові слова: виховна діяльність, моніторинг, управління, заклад вищої освіти, кваліметрична модель, якість виховної діяльності.

ВСТУП

У сучасному українському суспільстві відбуваються складні процеси, що обумовлені воєнно-політичними й соціально-економічними перетвореннями. Ці зміни не можуть залишатися непомітними для системи освіти України, у тому числі й в управлінні закладами вищої освіти.

За сучасних умов визріла об’єктивна необхідність створення адекватної завданням освітньої галузі системи аналізування та прогнозування, яка дозволить відстежувати освітні й управлінські процеси в динаміці та взаємозв’язку. Цю проблему може розв’язати моніторинг, суть якого полягає в синхронізації процесів спостереження, замірювання, отримання на цій

основі нових знань про стан об'єкта з подальшим моделюванням, прогнозуванням та прийняттям відповідного управлінського рішення. Від якості організації моніторингу суттєво залежить удосконалення виховної системи ЗВО, якій були би властиві гнучкість, демократизм, мобільність, здатність до самоорганізації.

Отже, актуальність означеної проблеми обумовила вибір теми нашого дослідження: «Удосконалення управління виховною діяльністю закладу вищої освіти засобами моніторингу».

Об'єкт дослідження: виховна діяльність закладу вищої освіти.

Предмет дослідження: моніторинг виховної діяльності закладу вищої освіти як функція управління.

Аналіз наукових джерел засвідчив певний інтерес до цієї проблеми. Так, суть, особливості освітнього моніторингу, його компоненти, засоби здійснення висвітлено в роботах В. Григораша, О. Мармази, В. Панасюка, І. Підласого, Т. Хлєбнікової, В. Циби та інших. Наукові дослідження О. Касьянової, Т. Лукіної, З. Рябової та інших присвячені моніторингу якості освіти в загальноосвітній школі; надбання М. Загірняка – аналізу моніторингу в освіті як науково-практичного феномена, а також деяким питанням моніторингу як форми пізнавальної діяльності. Моніторинг діяльності суб'єктів та об'єктів освітнього процесу досліджують науковиці Г. Єльникова та П. Матвієнко. Дослідник О. Биков у своїх працях порушує питання про концептуальні засади моніторингу виховання. О. Коберник досліджує педагогічний моніторинг як складову управління виховним процесом.

Отже, вивчення науково-педагогічної літератури засвідчило, що достатньо обґрунтовано специфіку виховної діяльності педагогів в умовах особистісно зорієнтованої парадигми освіти, описано технологію здійснення освітнього моніторингу, розроблено кваліметричні моделі оцінки роботи педагога за різними напрямами його діяльності. Але не запропоновано модель оцінки виховної діяльності закладу вищої освіти як основи моніторингових досліджень. Крім того, на практиці недостатньо узагальнено теоретичні доробки з питань проведення моніторингу для підвищення якості виховної діяльності й управління нею у ЗВО.

Разом із цим можна констатувати такі *суперечності:*

- між необхідністю підвищення якості виховної діяльності ЗВО й незавершеністю теоретичного розроблення відповідної процедури на основі кваліметричного підходу;
- між необхідністю вдосконалення моніторингу виховної діяльності ЗВО й незавершеністю теоретичного розроблення відповідної процедури на засадах програмно-цільового підходу.

Мета дослідження: теоретично обґрунтувати наукові засади моніторингу виховної діяльності ЗВО й на діагностичній основі розробити комплексно-цільову програму, метою якої є вдосконалення моніторингу як функції управління.

Відповідно до поставленої мети перед нами постали такі завдання:

1) визначити особливості виховної діяльності ЗВО й управління нею на сучасному етапі;
2) проаналізувати стан моніторингу виховної діяльності ЗВО;
3) розробити комплексно-цільову програму з удосконалення моніторингу виховної діяльності ЗВО, здійснити її експертизу та обґрунтувати впровадження.

Для виконання поставлених у дослідженні завдань було використано такі методи дослідження:

- *теоретичні:* аналіз і синтез, аналогія в поєднанні з індукцією, порівняння й узагальнення наукових джерел для визначення теоретичних засад моніторингу виховної діяльності ЗВО; метод теоретичного моделювання для визначення об'єкта, предмета; метод конкретизації та систематизації теоретичних знань для розробляння завдань дослідження;
- *емпіричні:* вивчення й узагальнення досвіду роботи ЗВО для виокремлення критеріїв і показників якості моніторингу виховної діяльності вишу; бесіда, спостереження, анкетування, тестування, метод експертних оцінок;
- методи математичної статистики та обробляння інформації: побудова рисунків і таблиць, упорядкування й унаочнення інформації та матеріалів.

Наукова новизна отриманих результатів дослідження полягає в тому, що *вперше*:

– уточнено особливості виховної діяльності закладу вищої освіти й управління нею в умовах повномасштабного російського вторгнення в Україну;

– розроблено кваліметричну модель оцінювання моніторингу виховної діяльності ЗВО;

– запропоновано комплексно-цільову програму з удосконалення моніторингу виховної діяльності ЗВО.

Набули подальшого розвитку ідеї програмно-цільового та кваліметричного підходів.

Практичне значення отриманих результатів полягає в упорядкуванні методик і методів вивчення стану моніторингу виховної діяльності ЗВО як важливої функції управління; розроблянні комплексно-цільової програми з удосконалення цього аспекту управлінської діяльності, яка може бути використана як базова для розробляння відповідних програм з урахуванням специфіки ЗВО, потреб і можливостей учасників освітнього процесу.

1. ТЕОРЕТИЧНІ АСПЕКТИ ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ВИХОВНОЮ ДІЯЛЬНІСТЮ ЗАКЛАДУ ВИЩОЇ ОСВІТИ ЗАСОБАМИ МОНІТОРИНГУ

1.1. Особливості виховної діяльності закладу вищої освіти й управління нею за сучасних

умов

Сучасна виховна діяльність в Україні насамперед має ту особливість, що здійснюється в занадто важких умовах воєнної агресії з боку російської федерації. Неможливо було уявити масштаби руйнацій, вторгнення, інформаційної війни на тлі фізичного вбивства українців – як військових, так і цивільного населення. Відтак маємо одночасно розв'язувати проблему підготовки педагогічних кадрів, оновлення методичних матеріалів, розроблення практикумів і тренінгів щодо здійснення основного напряму виховання – національно-патріотичного, та його складника – військово-патріотичного. Таке завдання зараз є і буде лишатися головним на найближчі роки.

Актуальними через війну стають не тільки проблеми формування справжнього патріотизму, розвитку любові до Батьківщини, готовності захищати її, бути вірними її громадянами, урахування культурно-історичної складової в освітньому процесі, закріплення європейських цінностей у світлі євроінтеграції України, а й проблеми психологічної підтримки учасників освітнього процесу, компенсації освітніх втрат через війну, застосування інформаційно-комунікаційних технологій у виховній діяльності на територіях, наближених до лінії фронту, де освітній процес в оффлайн форматі призупинено.

Отже, найважливішими виховними завданнями на сучасному етапі розвитку країни є такі:

1) національно-патріотичне та військово-патріотичне виховання дітей, молоді, дорослих людей, які пишаються своїм українським походженням, своїм громадянством;
2) формування системи загальнолюдських і національних цінностей, серед яких головною цінністю є життя людини; розвиток особистості загалом і мультикультурний розвиток особистості зокрема, формування полікультурної компетентності, навичок культури добросусідства;
3) превентивне виховання, профілактика шкідливих звичок, асоціальної, деструктивної, адиктивної поведінки; здійснення психологічної підтримки учасників освітнього процесу, збереження ментального здоров'я вихованців, педагогів, батьків;
4) розвиток цифрової компетентності учасників освітнього процесу, формування єдиного цифрового освітньо-виховного простору закладу освіти;
5) розвиток медійної культури, комунікативної культури, спілкування в інтернет-просторі, формування навичок критичного оцінювання інформації;
6) розвиток культури поведінки в суспільно-громадських місцях, виховання відповідальності за результати навчання та праці, формування індивідуального почерку – індивідуального стилю; створення умов для самореалізації вихованців;

7) розвиток цифрової компетентності керівників освітніх організацій, педагогів, батьків, осіб, які здійснюють виховний вплив на підростаюче покоління.

Окреслимо виклики, які постають у процесі виконання зазначених виховних завдань:

1) створення умов для повернення в Україну дітей і молоді, які змушені були покинути країну через військову агресію рф; повернення дітей і підлітків, яких було насильно депортовано з України до рф;
2) низький рівень розвитку навичок спілкування, говоріння через обмежені можливості спільного проведення дозвілля, надання переваги цифровим засобам взаємодії (краще написати, ніж вимовити);
3) загроза психічному здоров'ю через постійний стрес; погіршення фізичного здоров'я (гіподинамія, в'ялість, поганий зір, порушення осанки, ожиріння тощо) через відсутність необхідного обсягу рухливої активності;
4) легка доступність дітей і молоді до так званого «руйнівного контенту» – інформації, сайтів, ресурсів, що містять насильство, жахи, розвивають фобії, агресивність, неприязнь до людей за певними ознаками;
5) знецінення соціальних зв'язків як таких через втрату справжньої суті таких понять, як «дружба», «друг», «колектив»;
6) загроза негативного впливу соціальних мереж, а саме деструктивних челенджів, флешмобів, нав'язування деструктивної колективної поведінки, не обмеженої фізичним простором, яка спотворює справжні цінності, у тому числі знецінює людське життя;
7) брак часу на здійснення суто виховних заходів через необхідність дотримання санітарно-гігієнічних норм щодо організації освітнього процесу засобами дистанційних технологій *(О. Є. Гречаник, 2020)*.

Визначення мети й головних завдань виховної діяльності, окреслення можливих викликів, що стають загрозою на шляху їх досягнення, уможливлюють визначення основних підходів до виховної діяльності (акмеологічний, аксіологічний, компетентнісний, особистісно зорієнтований, діяльнісний, системний) і розроблення на діагностичній основі конкретних планів виховної діяльності з урахуванням конкретних умов виховання.

Розглянемо специфіку виховної діяльності вишу та представимо структуру виховної діяльності ЗВО – відповідно до критерію послідовності етапів і відповідних педагогічних дій:

1) удосконалення знань, норм і правил поведінки. Це перший етап входження в систему виховного впливу ЗВО, на якому діють норми, правила, особливості життєвої поведінки. Людина (студент) стає членом певної соціальної системи (студентського колективу), де

вже діють певні правила, норми, яких їй (йому) доведеться дотримувати;

2) розвиток почуттів (стійких емоційних ставлень людини до явищ дійсності). Вони сприяють трансформації певних дій особистості зі сфери розумового сприймання у сферу емоційних переживань, що робить їх стійкими, та активізації психічних процесів людини;
3) формування переконань (інтелектуально-емоційного ставлення суб'єкта до будь-якого знання як до істинного (або неістинного). Переконання, що ґрунтуються на істинних знаннях, будуть, з одного боку, своєрідним мотивом діяльності, а з другого – «стрижнем» поведінки особистості. Тому виховання молоді і є формуванням у неї психологічного «стрижня», без якого особистість буде безвольною, позбавленою власного «Я»;
4) розвиток умінь і звичок поведінки. Розвиток умінь (засвоєного способу виконання дій, основаного на сукупності набутих знань і навичок) і звичок (схильності людини до відносно усталених способів дій) потребує поступовості й систематичності вправляння, посильності та доцільності поставлених вимог, їх відповідності рівню розвитку здобувачів вищої освіти. Воно пов'язане з активною діяльністю особистості у сфері реальних життєвих ситуацій.

У нашій країні можна схарактеризувати загальну мету виховання у вищій школі через систему виховних завдань, які об'єднані в напрями виховної діяльності: політичне, національно-патріотичне, сімейне, мовне, трудове, екологічне, моральне, професійне, розумове, фізичне тощо *(Т. Виноградова, 2016; І. Дудка, 2015; В. Лозова, Г. Троцко, 2002).*

Парадигма виховання у ЗВО має бути спрямована на формування системи моральних і естетичних цінностей людини-патріота, громадянина, професіонала, носія культури, різнобічний розвиток індивідуальності, створення внутрішньої потреби в самовдосконаленні, в основі якої знаходяться:

- ідея самовизначення особистості (формування культури життєвого самовизначення людини);
- ідея спрямування виховання на особистість (у центрі уваги – особистість здобувача освіти, її індивідуальні нахили, інтереси, своєрідність характеру);
- ідея спільної діяльності викладачів і студентів (тільки у творчому співробітництві здобувач утримує необхідне керівництво);
- ідея колективної спрямованості (переосмислення принципу «виховання в колективі й через колектив»);
- ідея добровільності (без власної доброї волі здобувачів не можна втілити жодні ідеї виховання) *(О. Попова, А. Денисенко, С. Васильєва, 2021; І. Репко, 2015; С. Сисоєва, 2000)*.

З огляду на зміни в суспільно-політичному, громадському житті необхідно чітко визначити основні принципи виховання у вищій школі. Ними можуть бути такі, наприклад:

- принцип національної свідомості – формування національної ідентичності українця, розвиток особистості здобувача вищої освіти відповідно до інтересів держави Україна, усвідомлення культурно-історичної спадщини Українського народу, знання його історії, традицій, готовність до відстоювання незалежності, захисту кордонів і конституційного устрою;
- принцип акмеологічний – створення найкращих умов для особистісного та професійного розвитку здобувача вищої освіти;
- принцип особистісної орієнтації виховання – визнання й урахування в освітньому процесі індивідуально-психологічних особливостей його учасників;
- принцип науковості – використання в освітньому процесі досягнень сучасної науки – у технологіях, змісті, методиці, управлінні тощо;
- принцип перспективності та безперервності виховання;
- принцип виховання в діяльності та спілкуванні;
- принцип особистої відповідальності;
- принцип стандартизації – випускник ЗВО має відповідати стандартам вищої освіти та галузевим стандартам, наприклад стандарту керівника закладу загальної середньої освіти (ЗЗСО); стандарту керівника закладу дошкільної освіти (ЗДО) тощо;
- принцип інтеграції професійної підготовки майбутнього фахівця, розвитку його ціннісних орієнтацій, наукової, суспільної та навчальної діяльності.

1.2. Технологія моніторингу виховної діяльності закладу вищої освіти

Дефініцію «технологія» розглядаємо як послідовність певних кроків.

Мета моніторингу виховної діяльності – виявити потенційний ресурс виховання у вищій школі й розробити стратегію його реалізації. Ми погоджуємося з науковцями, зокрема З. Рябовою, які визначають моніторинг виховної діяльності як функцію управління, що передбачає систематичне й системне збирання, обробляння, подальше використання отриманих результатів виховання задля коригування мети й завдань виховної роботи *(З. Рябова, 2018)*.

Об’єктами моніторингу виховної діяльності в закладі вищої освіти може бути обрано:

- розвиток особистості студента й формування його новотворів у процесах самопізнання, самовиховання, самоствердження, самовизначення, саморегуляції, самоактуалізації й самореалізації, у т.ч. професійної;
- розвиток спілкування й особливості колективу студентської групи;

- створення виховного середовища ЗВО загалом і кожної студентської групи зокрема;
- діяльність усіх учасників освітнього процесу;
- соціально-педагогічна підтримка й соціальний захист здобувачів освіти;
- розвиток мотиваційної сфери студентів;
- розвиток пізнавальної сфери студентів;
- формування Я- Концепції кожного здобувача освіти;
- рівень вихованості студента, рівень сформованості його ціннісних орієнтацій як інтегративна особистісна характеристика *(О. Ішутіна, 2018; В. Мартинюк, 2023; О. Попова, 2021; В. Ткаченко, 2023; А. Харківська, 2014)*.

Моніторинг виховної діяльності передбачає діагностування кількісних і якісних показників, що дають можливість визначити стан і тенденції розвитку виховної системи ЗВО *(О. Темченко, 2019)*.

Системоутворювальною метою моніторингу якості виховної діяльності ЗВО є прогнозування подальшого розвитку виховної системи ЗВО, його освітнього середовища.

На нашу думку, показниками результативності виховної діяльності є створення сприятливого мікроклімату, збагаченого освітнього середовища ЗВО, стан здоров'я студентів, рівень їх вихованості, рівень морального, культурного розвитку здобувачів, рівень соціально-психологічного розвитку особистості здобувача (здатність співпрацювати, взаємодіяти, працювати в команді, пропонувати ініціативи, відповідати за прийняті рішення), дисциплінованість, суспільна активність, ставлення до праці, професійних обов'язків, наявність правопорушень, зайнятість у кружках і секціях, головні успіхи й досягнення студентів у різних видах діяльності, рівень сформованості студентських колективів, робота студентського самоврядування – ЗВО та окремих колективів, ступінь задоволеності виховною роботою всіх учасників освітнього процесу, результати роботи куратора щодо самоосвіти та професійного зростання, розвитку педагогічної майстерності *(О. Гречаник, О. Борисенко, 2023)*.

У процесі моніторингу слід обов'язково спиратися на визначені ЗВО місію, візію, стратегічну мету, стратегічні завдання – задля того, аби досягти визначеного образу випускника саме цього ЗВО.

Розроблення системи моніторингу виховної діяльності ЗВО припускає два основні етапи: аналітико-прогностичний та організаційно-технологічний.

Перший етап включає такі послідовні дії:

- осмислення предмета освітнього моніторингу, тобто того, що саме будуть відслідковувати в освітньому (виховному) процесі (напрями освітнього моніторингу);

- визначення критеріїв (або коректування критеріїв, запропонованих у програмі виховання, за якою працює освітня установа), за якими відслідковують результати освітнього процесу (складання критеріальної мапи освітнього моніторингу);
- розподіл того, що й ким буде вивчатися, узгодження змісту діагностичних актів, проведених викладачами, працівниками психолого-акмеологічної служби, куратором тощо (програма освітнього моніторингу);
- вибір методів вивчення здобувачів освіти, діагностичних методик і визначення (узгодження з іншими фахівцями) часу діагностичних актів;
- розроблення і визначення форм аналізу й фіксації результатів освітнього моніторингу.

На другому етапі освітнього моніторингу здійснюють такі дії:

- здійснення освітнього моніторингу на практиці, координація дій усіх фахівців;
- організація навчання й обміну досвідом між кураторами студентських груп, лідерами студентського самоврядування, науково-педагогічними та педагогічними працівниками, психологами, акмеологами, кар'єрними радниками й іншими фахівцями щодо змісту, методів діагностування, оцінювання, прогнозування ходу й результатів виховного процесу;
- проведення нарад, педагогічних консиліумів щодо аналізу отриманих даних, формулювання конкретних висновків і завдань, щодо рефлексії діяльності науково-педагогічних працівників тощо.

За своєю структурою моніторинг виховної діяльності ЗВО містить 4 елементи:

1) безпосереднє спостереження за виховною діяльністю;
2) оцінювання стану виховної діяльності;
3) прогнозування тенденцій розвитку виховної системи й кожного її елемента;
4) формулювання пропозицій із метою закріплення позитивних результатів й гальмування негативних процесів.

Отже, першим елементом моніторингу виховання є спостереження. Так, у моніторингу й діагностуванні виховання використовують, як правило, систематичне спостереження. Його ознаками виступають фіксація побаченого, регулярність проведення впродовж окресленого. Такий метод дозволяє виявити динаміку подій – позитивну, негативну чи статику.

У ході спостереження відбувається вивчення стану виховання. Вивчення – насамперед процес отримання якоїсь інформації. Із педагогічної точки зору, це не тільки одержання, але й спеціальний відбір інформації з метою її використання в певних педагогічно значущих цілях.

Якщо розчленувати процес вивчення, то він містить у собі два етапи:

1) отримання первинної інформації про суб'єктів виховання, тобто здійснюється така функція вивчення, як дізнавання. Суть дізнавання – відтворення й цілісне представлення найбільше характерних зовнішніх проявів;

2) перероблення інформації, її вторинне використання, тобто розпізнавання або приведення інформації в стан, що дозволяє співвіднести отримані дані із практичною діяльністю. Дізнавання дає можливість уявити собі загальний образ об'єкта, окремі його сторони, у той час як через розпізнавання встановлюють зв'язки між усіма його сторонами, їх взаємозумовленість, визначають особливості внутрішніх і зовнішніх відносин і характер.

Другий елемент моніторингу – оцінка стану виховання. Це уточнювальна стадія діагностики. Здійснення оцінки стану виховання дає можливість зрозуміти, який зміст схований за зовнішніми формами, які причини, мотиви, що детермінували виникнення зовнішніх ознак: «У діагностиці розвитку завдання дослідника полягає не тільки у встановленні відомих симптомів і перерахуванні їх або систематизації, і не в угрупованні явищ за їхніми зовнішніми, подібними рисами, але винятково в тому, щоб за допомогою розумового оброблення цих зовнішніх даних проникнути у внутрішню сутність процесів розвитку» *(В. Міхеєв, 2010)*.

Не можна не відзначити, що перші два компоненти моніторингу виховання – вивчення його стану шляхом безпосереднього спостереження й оцінка цього стану – досить широко досліджені в рамках теорії педагогічної діагностики (діагностики виховання).

Про науковий рівень діагностики можна говорити в тих випадках, коли діагностичне розпізнавання спрямоване на розкриття внутрішніх закономірностей розвитку особистості, на аналіз науково обґрунтованих ознак, показників, критеріїв. Що стосується виховання, то в цей час складно вирішувати питання наукової діагностики та пов'язаних із цим проблем, наприклад, морального виховання особистості, тому що об'єктивно немає повного опису норми й відхилень від неї. Труднощі діагностики пояснюються також складністю вивчення людини, групи, педагогічної діяльності.

Діагностичний рівень інформації виникає в тих випадках, коли її обсяг, якісна структура дають можливість здійснити кількісний і якісний аналіз.

Найважливішою умовою якісного діагностування й оцінювання виховання в процесі його моніторингу є інтерпретація й операціоналізація понять, зіставлення теоретичних положень із емпіричними даними з метою наукового обґрунтування діагностичних і прогнозованих результатів.

У педагогічній науці застосоване загальнонаукове положення щодо розкриття змісту поняття оцінювання. Воно може бути повним тільки в тому випадку, якщо його інтерпретація

ведеться у двох напрямках: зіставлення цього поняття з іншими поняттями (теоретична інтерпретація поняття) і зіставлення його з даними спостереження, тобто з емпіричними даними (емпірична інтерпретація поняття).

Емпірична інтерпретація понять являє собою специфічну процедуру пошуку емпіричних значень теоретичних термінів.

Прямої емпіричної інтерпретації, через «правила позначення», зазнають не всі елементи теоретичної системи, а тільки окремі терміни. Інші терміни одержують непряму теоретичну інтерпретацію завдяки установленню логічних зв'язків із безпосередньо тими, що інтерпретують.

Одним із «правил позначення» є операціональне визначення – це розкриття значення теоретичного поняття через вказівку тієї експериментальної операції, результат якої доступний емпіричному спостереженню або виміру, свідчить про наявність явища, вираженого в понятті. У найпростішому випадку – це вказівка емпіричного показника, що свідчить про наявність або відсутність явища, вираженого в теоретичному понятті.

Для кожного поняття можна зазначити емпіричні показники й систему дослідницьких засобів для їхнього фіксування. Наприклад, емпіричний показник ціннісних орієнтації – думка – фіксується за допомогою опитування (інтерв'ю, анкети), а показник ініціативності – кількість раціоналізаторських пропозицій – фіксується шляхом прямого підрахунку. Отже, вибір емпіричного показника залежить як від поняття, яке інтерпретують, так і від тих дослідницьких засобів, які має дослідник *(І. Кіндрат, 2013; Л. Козак, 2018)*.

Інтерпретація й операціоналізація понять у моніторингу виховання залежать від значень, вкладених у поняття «виховання», які тим самим визначають характер спостереження й оцінки стану виховної діяльності.

Щодо третього елементу моніторингу виховання – прогнозування розвитку виховання – слід зазначити, що процес педагогічного прогнозування, який входить до моніторингу виховання, складається з декількох операцій, перша й основна з яких – вибір цілей і завдань прогнозування. При цьому слід виходити як із загальних методологічних позицій, так і з особливостей конкретної ситуації.

Педагогічний прогноз може бути сприятливим, несприятливим, сумнівним, але не може бути безнадійним. У центрі уваги моніторингу мають бути позитивні тенденції. Саме від них має йти відлік до тенденцій негативних, щоб визначати умови, за яких позитивні елементи будуть переважати над негативними. Передбачення боротьби позитивних і негативних тенденцій має сполучатися з передбаченням результатів активного педагогічного втручання в цей процес.

Під час підготовки прогнозу враховується значущість прогнозованих об'єктів, яка визначається не стільки питомою вагою певного явища, скільки його положенням у системі причинно-наслідкових зв'язків. Такий розподіл об'єктів прогнозування за значущістю допомагає виявити тенденції розвитку об'єктів прогнозування, що враховують у процесі визначення головних параметрів прогнозу.

Визначення значущості факторів, що формують основні тенденції розвитку виховання, вимагає вивчення їх стійкості. Стійкість, у свою чергу, характеризується, по-перше, тривалістю періоду розвитку об'єкта до моменту прогнозування, по-друге, природою самого об'єкта, по-третє, роллю зовнішніх умов, які можуть вплинути на об'єкт у процесі прогнозування, а також у наступний період.

Стійкість може бути як статичною, так і динамічною. Статична стійкість характеризує малу рухливість зовнішніх форм існування педагогічного явища (наприклад, постійні симпатії або антипатії людини до окремих членів родини, до товаришів по студентській групі за стійкого сприятливого або несприятливого положення здобувача в системі цих відносин). Динамічна стійкість означає легку мінливість зовнішніх форм існування об'єкта в разі стійкості його внутрішньої природи (наприклад, зміна партнерів по спілкуванню, більша емоційна мобільність у відносинах із ними за умови сталості інтересів, мотивів вчинків).

Прогнозування виховання студентів передбачає облік спрямованості розвитку тих факторів, які визначають характер виховної діяльності, підґрунтя, сукупності зовнішніх факторів, що оточують об'єкт прогнозування.

У моніторингу виховання виділяють три види прогнозів: найближчий, актуальний, перспективний *(О. Гречаник, 2020; А. Харківська, 2014)*. Зміст найближчого прогнозу полягає в пророкуванні можливих дій об'єктів вимірювання. Актуальне прогнозування націлене на пророкування спрямованості їх взаємодії. Суть перспективного прогнозу полягає в пророкуванні провідних тенденцій розвитку виховної діяльності.

Експертна оцінка отриманого прогнозу здійснюється у двох формах: вербальній та письмовій. Під вербальною мають на увазі усне опитування компетентних осіб (батьків, педагогів і т.д.) про тенденції виховання й розвиток особистості студента, процесів і явищ. Збирання оцінок експертів можна проводити як індивідуально, так і в ході групового обговорення.

Четвертий елемент моніторингу – складання рекомендацій за результатами зібраної інформації.

Планування розвитку позитивних і попередження виявлених негативних процесів – завершальний етап моніторингу виховання. План відрізняється від прогнозу насамперед тим, що він являє собою не просте передбачення майбутнього, але й програму дій.

Головна мета планування полягає в розвитку всього того, що створює оптимістичну основу прогнозу, припускає активне педагогічне втручання у виховний процес, тобто всілякий розвиток позитивних тенденцій, які не тільки блокують, але й долають недоліки.

Слід сказати, що в моніторингу виховання етап планування розвитку позитивних і попередження виявлених негативних процесів найчастіше здійснюється не в конкретних запланованих заходах, а у формулюваннях практичних рекомендацій суб'єктам виховання щодо подолання негативних тенденцій.

Завдання діагностичної діяльності визначають вибір методів дослідження.

До методів вивчення якості виховної діяльності в освітній організації відносять такі: діагностичні, експериментальні, не експериментальні та формувальні *(І. Кіндрат, 2013; Л. Козак, 2018; В. Кульчицький, 2021; В. Лозова, Г. Троцко, 2002; О. Попова, 2021)*.

Проаналізувавши різні методи вивчення якості виховної діяльності в освітній установі, ми дійшли висновку, що одним з оптимальних методів вивчення рівня сформованості особистісних якостей, системи ціннісних відносин у студентів є метод анкетування. Анкетування являє собою методичне приймання одержання інформації за допомогою складених відповідно до певних правил систем питань. За допомогою анкетування педагог одержує матеріал для встановлення суджень і особистісних якостей здобувачів.

Перевагами анкет є: масовість обстеження; висока швидкість отримання даних; простота оброблення даних; можливість використання методів статистичного аналізу.

Уважаємо за необхідне зазначити, що предметом особливої уваги кураторів студентських груп мають бути не розрізнені окремі якості чи риси характеру студента, а його цілісна особистість та спрямованість.

Діагностика рівня вихованості здійснюється методом експертної оцінки *(З. Рябова, 2018; T. Khliebnikova, 2020)*. Суть методу полягає в колективному оцінюванні групою експертів (викладачами й кураторами, які працюють із певним студентом) особистості того, якого навчають, його розвитку й вихованості. Підсумкова оцінка складається шляхом статистичного оброблення анкет, запропонованих кожному експертові. Параметри, за якими ведеться оцінювання якості виховання, на кожному етапі виховання у ЗВО, можуть варіюватися залежно від соціуму, у якому перебуває певна освітня установа, від ступеня зрілості педагогічного й студентського колективу. Результати експертизи можуть бути зіставлені зі стандартами виховання, зафіксованими в концепції виховання освітньої установи.

Інструментарій моніторингу – це засоби, які використовують у процесі його проведення, та складники. Ними можуть бути різноманітні види аналізу, у тому числі статистичні, тематичні перевірки, анкетування, інтерв'ю, тестування, опитування, аналіз документації ЗВО, дані самооцінювання та самоспостереження, інституційного аудиту тощо.

Щодо складників моніторингу, то ними є такі, як об'єкт моніторингу, зазначені параметри розвитку, критерії та показники розвитку, технологія здійснення контролю, засоби коригування й регулювання.

Основним фактором у створенні інструментарію є розроблення моделей оцінювання об'єктів моніторингу.

У разі створення таких моделей, як правило, виділяють:

- параметри, які відповідають цілям діяльності об'єкта;
- фактори, що впливають на досягнення мети;
- критерії, що деталізують кожний фактор, відповідно до освітніх завдань, як окремого ЗВО, так і регіону загалом.

Із метою одержання об'єктивних результатів визначають коефіцієнт кожного критерію. Цей коефіцієнт являє собою бальну оцінку в частинах одиниці й може збільшуватися або зменшуватися залежно від зміни пріоритетних напрямків у діяльності ЗВО *(Г. Єльникова, 2004, 2017)*.

Для ефективної організації проведення моніторингу на рівні ЗВО доцільно використовувати такий алгоритм.

1. Наказом ректора ЗВО затвердити склад робочих груп із проведення (супроводу) адміністративного, педагогічного, студентського моніторингу.

   До складу робочих груп включають таких представників:

- представники адміністрації ЗВО;
- представники органів самоврядування ЗВО;
- керівники структурних підрозділів – факультетів, кафедр, відділів, лабораторій;
- працівники психолого-акмеологічної служби;
- представники наглядової ради ЗВО.

2. Внести (у разі потреби) доповнення або зміни в представлені моделі відповідно до статусу та пріоритетних напрямів діяльності ЗВО.
3. Ознайомити колектив ЗВО (викладацький, студентський) із порядком проведення моніторингу, факторно-критеріальними моделями, технологією оцінювання.
4. Для одержання достовірної інформації від різних категорій учасників освітнього процесу, визначення якості виховної діяльності розробити анкети, опитувальники, діагностичні

картки, завдання, тести і т. д.

5. У строки, визначені адміністрацією ЗВО, провести моніторингові дослідження.
6. Обробити й проаналізувати отримані дані.
7. На основі отриманих результатів аналізу розробити моделі корекційної діяльності учасників освітнього процесу на всіх рівнях («студент – студент», «викладач – студент», «викладач – адміністрація» і т. д.).
8. Обговорити підсумки моніторингу на розширеному засіданні Вченої ради ЗВО.
9. Довести результати моніторингу до свідомості учасників ОП та громадськості.

Для розв'язування виявлених проблем необхідно розробити план заходів, або цільовий проєкт, або комплексно-цільову програму.

2. ПРАКТИКА ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ВИХОВНОЮ ДІЯЛЬНІСТЮ ЗАКЛАДУ ВИЩОЇ ОСВІТИ ЗАСОБАМИ МОНІТОРИНГУ

2.1 Дослідження стану моніторингу виховної діяльності Харківського національного педагогічного університету імені Г. С. Сковороди

Основними завданнями аналізу стану моніторингу виховної діяльності ХНПУ імені Г. С. Сковороди як управлінської проблеми були визначені такі:

1) з'ясувати кількісний і якісний склад науково-педагогічних працівників, які забезпечують освітній процес у виші;
2) оцінити готовність науково-педагогічних і педагогічних працівників закладу до проведення моніторингу виховної діяльності;
3) визначити напрями виховної діяльності вишу;
4) здійснити оцінку стану моніторингу виховної діяльності ЗВО як управлінської проблеми.

Аналіз стану проблеми здійснювався шляхом:

- вивчення внутрішньої документації ЗВО;
- аналізу відгуків студентів і випускників про задоволення роботою освітнього закладу;
- огляду та оцінювання матеріально-технічної бази ЗВО;
- вивчення та аналізу управлінських рішень, рішень Вченої ради, засідань вчених рад факультетів і науково-методичних комісій та інших управлінських структур вишу;
- відвідування навчальних занять і виховних заходів;
- огляду та оцінки наукового, навчально-методичного забезпечення освітнього процесу;
- аналізу кадрового складу;
- співбесіди з керівниками, науково-педагогічними та педагогічними працівниками, здобувачами освіти, громадськістю;
- анкетування, опитування, спостереження тощо.

Матеріали аналізу містять письмовий звіт, таблиці, діаграми, діагностичні матеріали, матеріали анкетування тощо.

Мікродослідження № 1. Кадрове забезпечення освітнього процесу у ЗВО.

Мета: з'ясувати якісний і кількісний склад працівників ЗВО.

Відповідно до мети дослідження було проаналізовано документацію, штатний розклад, особові справи науково-педагогічних і педагогічних працівників.

2024 року ХНПУ імені Г. С. Сковороди святкуватиме 220-річчя від дня заснування. Нині університет – це потужний інноваційний заклад освіти, флагман освіти Слобожанщини, який має за мету найближчим часом підвищити рейтинги серед ЗВО країни. Так, за даними 2023 року ХНПУ посів 52 місце серед усіх ЗВО країни та 1-е місце серед педагогічних вишів України. Із 209 ЗВО університет посідає 25 місце за індексом Гірша в Гугл-Академії.

Чисельність здобувачів освіти всіх рівнів і форм здобуття освіти – 6000 осіб.

Кількість факультетів – 10, інститутів – 1 (Інститут післядипломної освіти і менеджменту).

Кількість кафедр – 43.

В університеті здійснюється підготовка фахівців першого-четвертого рівнів вищої освіти, від бакалавра до доктора наук. Зокрема, за 38 спеціальностями здобувають освіту магістри – 45 освітніх програм, аспіранти й докторанти – за 10 освітніми програмами.

Освітній процес забезпечують 426 науково-педагогічних і 18 педагогічних працівників, серед яких: 424 – на постійній основі; 92 – доктори наук; 74 із них – професори; 258 – кандидати наук, із них 189 – доценти (рис. 2.1). Загалом 82,6 % працівників мають наукові ступені та звання.

Університет очолює ректор Бойчук Юрій Дмитрович, обраний трудовим колективом 03 листопада 2020 року, доктор педагогічних наук, професор, член-кореспондент Академії педагогічних наук України.

Заклад освіти має унікальні традиції та сформовану систему виховної роботи.

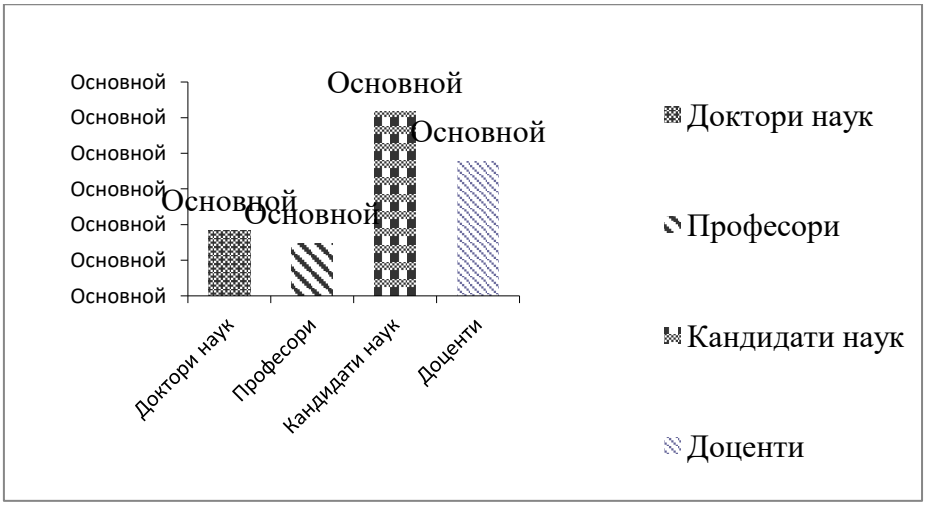


Рис. 2.1. Склад працівників, які забезпечують освітній процес у ЗВО

Отже, результати дослідження свідчать про високий рівень якості кадрового складу працівників, які забезпечують освітній процес у закладі освіти.

Мікродослідження №2. Оцінка готовності науково-педагогічних і педагогічних працівників закладу до проведення моніторингу виховної діяльності.

Мета: вивчення рівня готовності педагогічних працівників до проведення моніторингу виховної діяльності.

Для оцінки готовності працівників ЗВО до проведення моніторингу нами було проведено анкетування. Системний аналіз проведеного анкетування дозволив виявити проблеми в здійсненні педагогічного моніторингу в професійній діяльності науково-педагогічних і педагогічних кадрів.

Аналіз результатів анкетування респондентів засвідчив їх ставлення до проблеми моніторингу та значущість моніторингових досліджень. Це підтверджують такі показники: 92 % опитаних уважають, що зібрана інформація важлива для адміністрації ЗВО, науково-педагогічних і педагогічних працівників (відповідно НПП та ПП), студентів.

З отриманих даних виходить, що більшість НПП і ПП мають високий рівень мотивації до діяльності й уважають себе рівноправними суб'єктами моніторингових досліджень.

Отже, проблеми мотивації НПП і ПП до діяльності щодо здійснення освітнього моніторингу виховної діяльності не було виявлено.

У ході анкетування було також виявлено, що 95 % респондентів вільно оперує поняттям «моніторинг», 3 % – не мають чіткого уявлення про суть і зміст поняття «моніторинг», 2 % – не визначилися з відповіддю. 95 % респондентів точно визначають основну мету моніторингу виховної діяльності й уважають це необхідним і важливим за сучасних умов – військової агресії рф проти України (рис. 2.2).

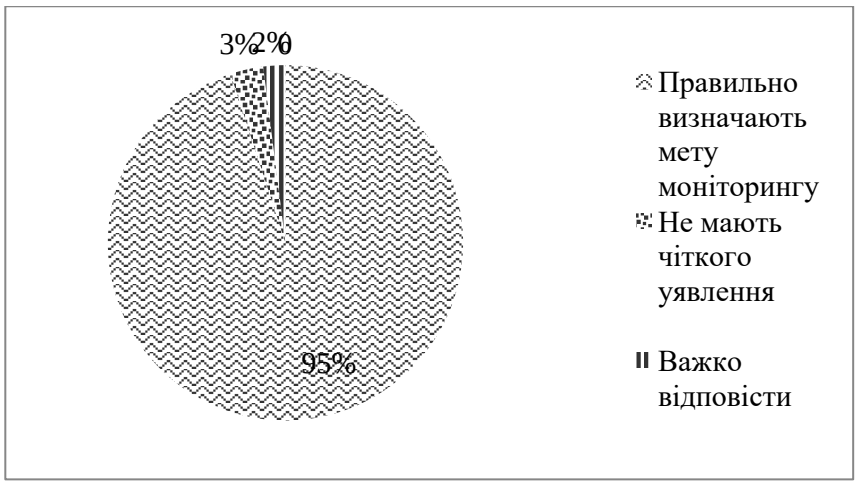


Рис. 2.2. Теоретична готовність НПП і ПП до моніторингу виховної діяльності

Таким чином, у ході анкетування не була виявлена проблема теоретичної готовності НПП і ПП до проведення моніторингу виховної діяльності.

Практична готовність працівників до здійснення моніторингу виховної діяльності визначалася на основі самооцінювання. Нами було проаналізовано відповіді респондентів на запитання: «Якими вміннями для здійснення моніторингових досліджень Ви володієте?». Так, 95 % респондентів володіють уміннями структурування та аналізу спостережень; 82 % – узагальнювати та систематизувати інформацію; 71 % – визначати напрями розвитку суб'єктів моніторингу на основі зібраної інформації (рис. 2.3).

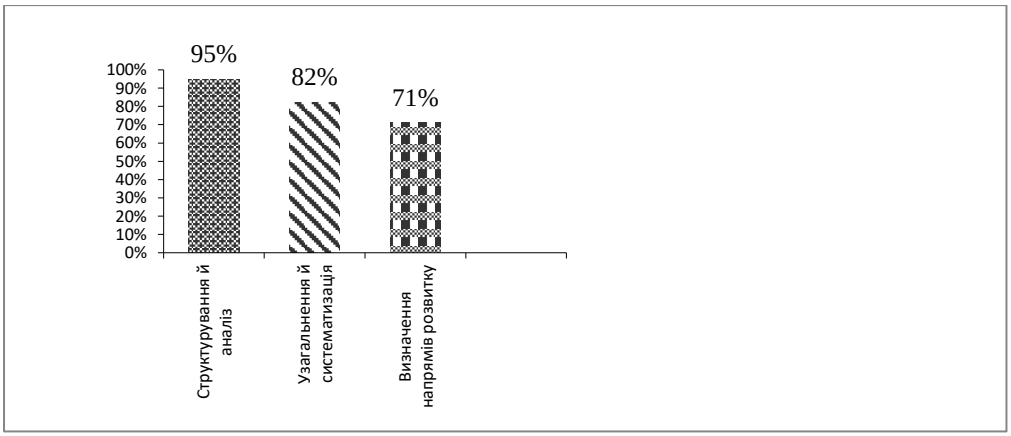


Рис. 2.3. Практична готовність НПП і ПП до моніторингу виховної діяльності

Результати самооцінювання відображають високий рівень (більше 70 %) володіння НПП і ПП окремими вміннями щодо здійснення моніторингу виховної діяльності. На підставі вище зазначеного можна стверджувати, що більшість працівників вишу практично готові до проведення моніторингу виховної діяльності. Однак для тих категорій працівників, які зазначили, що не мають розвинутих умінь аналізувати, узагальнювати інформацію чи визначати напрями розвитку суб'єктів виховання, слід передбачити теоретичні та практичні

форми роботи, спрямовані на оволодіння технологією проведення моніторингу виховної діяльності: практичні заняття, вебінари, майстерки тощо.

Мікродослідження № 3. Напрями виховної діяльності ЗВО.

Мета: визначити основні напрями виховної діяльності у ЗВО.

Виховна діяльність є невід'ємним складником освітнього процесу в ХНПУ імені Г. С. Сковороди. Період російської агресії проти України потребував від усіх учасників освітнього процесу переосмислення зробленого. Нормативно-правовою базою виховної діяльності в Університеті є: Конституція України, закони України «Про освіту», «Про вищу освіту», нормативні документи МОН України, Національна доктрина розвитку освіти України в XXI ст., Концепція національно-патріотичного виховання в системі освіти України, Стратегія національно-патріотичного виховання, накази ХНПУ, факультетські плани виховної роботи. Виховна робота спрямована на формування свідомих громадян України, забезпечення відповідних умов для самореалізації студентів, виховання внутрішньої культури майбутніх учителів, здатних нести знання школярам і зорієнтованих на продуктивну й ефективну взаємодію з іншими людьми.

Основними напрямами виховної діяльності в Університеті визначено такі: національно-патріотичне, громадянське, професійне, трудове, правове, мовне, мультикультурне, екологічне, валеологічне, художньо-естетичне, фізичне виховання.

Так, на нараді координаторів у лютому 2023 року було розглянуто плани виховної роботи на факультетах, проаналізовано й розроблено комплекти організаційно-методичних матеріалів для підтримки роботи кураторів факультетів із академічними групами, обговорено та скориговано завдання виховної роботи з урахуванням воєнного стану через російське вторгнення в Україну.

Через воєнний стан кураторами академічних груп було організовано та проведено бесіди зі здобувачами щодо питань безпеки охорони здоров'я та життєдіяльності у період воєнного стану, надано інформацію про активну діяльність Психологічної служби Університету (керівник – професор кафедри психологічної та педагогічної антропології І. Дорожко) у контексті надання психологічної підтримки здобувачам. До Психологічної служби мали та мають можливість звертатися як здобувачі, так і професорсько-викладацький склад, аби отримати необхідну психологічну допомогу, що особливо є затребуваним у сучасних реаліях.

Після продовження воєнного стану на території України кураторами академічних груп було проведено цикл годин спілкування на загальні теми: «Безпека під час воєнного стану» та «Психологічна підтримка під час воєнного стану». Також на факультетах відбувся

просвітницький онлайн-захід на тему «Інформування про ризики, пов'язані з мінами та вибухонебезпечними залишками війни (ІНРМ) для дорослих», яку провів Бирін Олександр Андрійович – фахівець з інформування мінної небезпеки Данської ради у справах біженців (Danish Refugee Council). Під час заходу слухачі ознайомилися з видами мін, основними типами травмування від мін, розглянули правила поводження з вибухонебезпечними предметами та переглянули інформативне відео з випробовувань різних видів мін. Здобувачі освіти з великим інтересом слухали фахівця з інформування мінної небезпеки та під час заходу мали можливість ставити гострі питання, на які одразу отримували ґрунтовні відповіді, адже онлайн-захід проходив у форматі відкритого діалогу.

31.01.2023 для викладачів та студентів Університету відбулася онлайн-зустріч зі співробітником Управління протидії кіберзлочинам у Харківській області – Максимом Сергійовичем Северіним,– яку було організовано за сприяння керівництва ХНПУ імені Г. С. Сковороди. Під час зустрічі доповідач представив слухачам проєкт «MRIYA», що спрямований на співпрацю кіберполіції України та волонтерів у протидії російським окупантам у медіа-просторі. Учасники зустрічі дізналися, що проєкт «MRIYA» протидіє російській агресії в Інтернет-мережі та блокує фейкові й проросійські ресурси.

29.06.2023 викладачі та студенти Університету на чолі з кураторами академічних груп відвідали онлайн-лекцію на тему «Ризики, що пов'язані з вибухонебезпечними предметами», яку провела представниця організації з розмінування Halo Trust Ukraine Євгенія Завада. Під час лекції слухачі ознайомилися з видами мін і розглянули правила поводження з вибухонебезпечними предметами.

Військовий конфлікт в Україні, безумовно, вніс свої корективи й окреслив пріоритетні напрями виховної роботи. З огляду на вище зазначене одним із найважливіших напрямів визнано роботу в медіа просторі. Так, постійно підтримується робота й регулярно оновлюється контент сторінок факультетів ХНПУ імені Г. С. Сковороди в соціальних мережах Facebook та Instagram.

У межах національно-патріотичного та громадянського виховання кураторами академічних груп факультетів упродовж 2023 року було проведено низку таких заходів:

- тематичний вечір «Українські зимові традиції»;
- тематична вітальня «Герої сьогодення» – до Дня Збройних Сил України;
- кураторські години до Дня пам'яті героїв Крут «Крути… Мужність і біль України», «Крути – символ українського патріотизму», перегляд фільму «Крути 1918»;
- кураторська година до Дня Соборності України;
- кураторська година до Дня пам'яті героїв Крут.

У межах професійного і трудового виховання кураторами академічних груп факультетів було проведено низку таких заходів: участь у заходах, присвячених святкуванню 300-річчя Г. С. Сковороди; тематичне засідання «Стежками Сковороди»; дискусійний клуб «Ритор»; проведення кураторських годин, тематичних бесід, наукових заходів, випуск стіннівок та організація літературних виставок; тематичний вечір «Дарунки Святого Миколая»; «Університет – моя родина»; зустріч ректора зі студентами-сиротами; усний журнал до Всесвітнього дня азбуки Брайля; засідання етнографічного клубу; Новорічні вечорниці; конкурс «Студент року – 2023» тощо.

Під час війни студенти Університету доєдналися до загального волонтерського руху й активно займаються цією діяльністю на різних напрямках. Волонтери університету систематично збирають та надсилають кошти для благодійного проєкту ХНПУ імені Г.С. Сковороди «Щасливі соняшники», що функціонує заради підтримки дітей з деокупованих територій. Також студенти Університету на чолі з викладачами протягом 2023 року систематично відвідували дітей з деокупованих територій та проводили для них різноманітні заходи.

Студенти Університету долучилися до донорського руху, який передбачає допомогу військовим і цивільним життєво необхідними препаратами з плазми крові.

Здобувачі успішно проходять курс підготовки інструктора з тактичної медицини базового рівня, отримують сертифікат інструктора з тактичної медицини Центру тактичної медицини «Схід» і навчають тактичної медицини представників Збройних Сил України, волонтерів, цивільних не тільки в Харкові й області, а й в інших областях нашої країни.

Створено волонтерський склад для гуманітарної допомоги людям із деокупованих територій, для поранених та підтримки різних військових підрозділів. Викладацький склад волонтерського загону «Злагода» організовує логістику гуманітарної допомоги за потребами військових частин, підрозділів поліції та ДСНС.

За звітний період до військових шпиталів було доставлено медичні інструменти та обладнання – інвалідні візки, милиці, перев’язувальні матеріали, ліки, памперси та пелюшки для важко поранених. Також забезпечуємо деякі відділення психічної лікарні, військовий госпіталь та лікарні м. Харкова, пгт Нова Водолага продуктами харчування: крупи, овочі, олія, різні смаколики.

Важливим і цікавим став для нас проект «Веселий соняшник» для дітей із деокупованих територій, який очолила проф. Анна Боярська-Хоменко. До творчого складу реабілітаційної групи педагогів увійшли Т. Довженко, С. Васильєва, О. Кін, О. Гуліч. Під час спілкування,

дозвілля з дітками волонтерська група викладачів здійснювала профорієнтаційну роботу. Результатом є вступ випускників 2023 року до нашого Університету.

Станом на зараз понад 50 викладачів нашого університету за свою волонтерську діяльність отримали подяки від БО «БФ “Харків з тобою”», волонтерської організації «Help army», від ХОДА та мера міста. Під час свята «Студент року» були нагороджені студенти-волонтери.

У межах правового виховання кураторами академічних груп факультетів було проведено низку таких заходів.

Заходи до Всесвітнього дня прав людини. Проведення тренінг-гри «Закон і Я».

Заходи до Міжнародного дня боротьби за ліквідацію расової дискримінації.

Бесіда-диспут «Щоб нація була здоровою» – до Міжнародного дня боротьби із зловживанням наркотиками та їх незаконним обігом.

Кураторська година «Права й обов’язки студентів України».

Кураторська година «Запобігання та протидія булінгу» – до Міжнародного дня протидії булінгу.

Участь у загальноміських та університетських заходах до Дня захисту дітей та до Дня молоді. Виготовлення подарунків дітям своїми руками «Подаруй любов дитині».

Правова виставка «Головний підручник життя» – до Дня Конституції України.

Бесіда з профілактики правопорушень і пропагування здорового способу життя щодо дотримання правил пожежної безпеки та правил безпеки руху.

Кураторська година, присвячена обговоренню основних положень Закону України «Про запобігання корупції».

Кураторська година на тему: «Про надання матеріальної допомоги особам, у яких пошкоджено майно. Про виплати міжнародних організацій родинам з дітьми та ВПО».

У межах мультикультурного виховання на факультетах було проведено такі заходи: віртуальна екскурсія «Мости релігій: синагога, костел, кенаса, церква, мечеть»; читацька конференція «Аспект виховання у творах дитячої літератури різних країн»; бесіда «Ми такі різні, але ми всі люди…»; кураторська година, присвячена французьким письменникам; флешмоб до Міжнародного дня боротьби за ліквідацію расової дискримінації; кураторська година на тему «Танці народів світу» – до Міжнародного дня танцю; кураторська година на тему «Полікультурна освіта в багатонаціональному середовищі»; виховна година «Чи вважаєте ви себе європейцями?» до Дня Європи в Україні; відвідування наукового музею «Ландау Центру» Харківського національного університету – до Міжнародного дня музеїв; участь у заходах до Міжнародного дня миру; проведення кураторської години «Мир і спокій

– дуже цінний для українців». Виготовлення голубів миру; перегляд вистав, відвідування віртуальних експозицій; участь у проведенні благодійних ярмарок на факультетах тощо.

Учасники Студентського парламенту активно беруть участь в організації студентських проєктів на рівні університету та окремих факультетів, є учасниками та переможцями різних студентських турнірів, конкурсів, олімпіад, гуртків, вебінарів, конференцій тощо.

Сьогодні Студентський Парламент ХНПУ імені Г. С. Сковороди налічує 14 постійних членів та 454 активних учасників із числа всіх здобувачів 1-го та 2-го рівнів вищої освіти.

Упродовж 2023 року здобувачі вищої освіти організовували, брали участь та були доповідачами на загальноуніверситетських, усеукраїнських і міжнародних заходах, створювали відеозвернення з нагоди окремих дат у календарі й організовували допомогу для студентів великої Сковородинівської родини.

Важливим осередком виховної діяльності в Університеті є культурно-мистецький центр. Його робота під час воєнного стану спрямована, перш за все, на духовно-патріотичне виховання студентської молоді, а також виявлення та розкриття талантів та обдарованості колективів, надання можливості реалізувати свій мистецький потенціал. Центр опановує нові форми роботи, які були реалізовані в заходах 2023 року та дали змогу продовжувати творчо-виховний процес за будь-яких умов перебування студентів і працівників центру.

Пріоритетною залишається концертно-волонтерська діяльність працівників центру та учасників творчих колективів, а також проведення університетських свят у форматі онлайн та наживо, участь у міських та обласних культурно-мистецьких заходах.

Невід’ємним складником виховної діяльності вишу є Музейний комплекс ХНПУ імені Г. С. Сковороди, що було створено на підставі рішення Вченої Ради Університету. Він є структурним підрозділом Університету.

Основними напрямами діяльності музейного комплексу в 2023 році, за якими велась робота зі студентами Університету й готувались низка проєктів історичного, краєзнавчого і музеєзнавчого напрямків, були такі:

- музеєзнавство;
- історико-краєзнавчий;
- історична біографістика;
- історія університету;
- історія України.

Адміністрацією музейного комплексу під загальним керівництвом проректора з навчально-виховної роботи доц. Н. Борисенко було запропоновано до реалізації низку онлайн проєктів, що дозволили проводити широкий спектр заходів історичного, краєзнавчого,

виховного та національно-патріотичного спрямування для студентів університету, викладачів, школярів шкіл міста й області, які перебувають в Україні та за її межами.

Зважаючи на сучасну суспільну ситуацію в країні, а також з огляду на значну кількість студентів, які в результаті війни виїхали за межі нашої держави, для здобувачів освіти були організовані віртуальні екскурсії, які ознайомлювали їх з історією та визначними архітектурними пам'ятками міст Європи – Праги, Відня та Кракова. У процесі екскурсій студенти отримали корисну інформацію про такі шедеври європейської архітектури, як Празький Град, Карлов міст, Собор св. Стефана, Вавельський замок тощо.

Важливе місце в роботі музейного комплексу займала подальша діяльність у межах започаткованого в 2022 році проєкту «Видатні українці». Цього року для студентів університету було проведено низку онлайн-заходів, у ході яких були представлені життєписи людей, які увійшли в історію України своїми героїчними вчинками та видатними науковими, суспільними та громадськими справами. Серед цих видатних особистостей – Тарас Шевченко, Микола Терещенко, Володимир Вернадський, Павло Скоропадський, Ігор Сікорський, Євген Патон, Іван Франко та ін.

Завдяки різноманітним джерелам інформації, роботі в онлайн-архівах та бібліотеках України і зарубіжних країн видатні історичні постаті України можна висвітлити для студентів у всій багатогранності образів.

Наступного 2024-го року керівництво музейного комплексу планує розширити рамки проєкту «Видатні українці» шляхом долучення до проєкту біографій видатних українських митців, спортсменів, громадських діячів та інших особистостей, які сприяли зміцненню й утвердженню нашої держави на різних етапах її існування.

Активно бере участь музейний комплекс і в заходах, присвячених історії Університету, знаменним датам і вшануванню людей, які зробили значний внесок в історію ХНПУ. Так, під загальним керівництвом проректора з навчально-виховної діяльності доц. Наталії Борисенко керівництвом музейного комплексу було започатковано серію заходів для першокурсників університету, присвячених видатному українському філософу і просвітителю Григорію Савичу Сковороді, чиє ім'я носить наш університет.

Під час проведення цих зустрічей в онлайн першокурсники знайомились із творчим спадком Сковороди, маловідомими фактами його біографії, подорожували історичними місцями України, де проходило життя та подорожі філософа. Також у межах цього проєкту студенти дізнавалися про сторінки історії Слобожанщини, становлення середньої та вищої освіти в Харкові й області у другій половині XVIII століття.

Дуже важливою компонентою в діяльності музейного комплексу є репрезентація студентам проєктів та заходів національно-патріотичного виховання, які присвячені безпосередньому вивченню й засвоєнню ними знань з історії України.

На початку 2023 року керівництвом музейного комплексу був підготовлений і презентований широкому студентському загалу віртуальний проєкт «Кольорова етнографія України». Була проведена робота з відбору філокартичних матеріалів і документів епохи з відкритих джерел, які ілюстрували побут, повсякденне життя та працю українців наприкінці XIX - початку XX століття. Цей проєкт викликав увагу студентів, було проведено декілька заходів з його презентації на різних факультетах університету.

Також у межах ознайомлення студентів з героїчним минулим української держави та її національними героями був створений та представлений студентській спільноті університету онлайн-проєкт з військової історії «Іван Сірко – видатний полководець України». У ньому на основі архівних матеріалів, праць відомих українських істориків зроблена спроба висвітлити багатогранну діяльність визначного військового діяча XVII століття, кошового отамана Запорізької Січі Івана Дмитровича Сірка.

Важливим проєктом музейного комплексу, який був започаткований 2023-го року, став проєкт «Архітектурні перлини України». Основним об’єктом уваги стали визначні пам’ятки архітектури, містобудування, садово-паркового будівництва, промислові й індустріальні об’єкти, які формують архітектурне обличчя різних областей нашої держави.

Також важливим аспектом діяльності музейного комплексу було питання професійного розвитку співробітників, здобуття ними нових знань. Протягом травня-червня 2023 року директор музейного комплексу опанував курс під керівництвом кандидата мистецтвознавства А. Арояна «Історія українського мистецтва», що був започаткований однією із культурно-просвітницьких організацій Полтавської області, та отримав багато корисної інформації з питань історії українського мистецтва. Отримані знання стануть у пригоді в процесі планування та реалізації нових історико-мистецьких проєктів музейного комплексу.

Щодо підсумків 2023 року, слід наголосити, що він був насиченим, хоча і непростим для музейного комплексу. Було створено й запущено в роботу сім нових історичних, краєзнавчих і музеєзнавчих проєктів, проведено понад 45 заходів для студентів Університету, школярів і студентів інших закладів освіти.

У вересні 2023 року в ХНПУ імені Г. С. Сковороди був створений Центр ветеранського розвитку.

Метою створення Центру ветеранського розвитку є надання комплексної (правничої, економічної, психологічної, логотерапевтичної та психокорекційної) допомоги військовослужбовцям, членам їх сімей і забезпечення їх ресоціалізації в соціумі.

Основними напрямами роботи Центру є такі.

Правничий напрям, який реалізується шляхом здійснення:

1) юридичного консультування (надання первинної правової допомоги) військовослужбовцям та членам їх сімей;
2) юридичного супроводу вирішення спірних питань військовослужбовців і членів їх сімей (для оформлення соціальної допомоги, звернення до суду, центрів надання адміністративних послуг тощо);
3) проведення онлайн/офлайн навчання (тренінгів) із питань:

- доступу до правосуддя;
- порядку реєстрації та користування функціональними можливостями системи «Електронний суд»;
- захисту житлових прав;
- захисту права на отримання соціальної допомоги;
- реалізації соціальних гарантій військовослужбовців;
- захисту права на працю;
- реалізації права на спадкування (оформлення спадкування);
- реєстрації власного бізнесу;
- пошуку місць для працевлаштування;
- пошуку грантових проєктів для учасників бойових дій та ветеранів;
- складання звернень до державних органів;
- отримання документів, що мають юридичне значення;
- основ юридичної відповідальності тощо;

4) проведення воркшопів за темами:

- мистецтво самопрезентації;
- формування резюме європейського зразка;
- лайфхаки для успішного проходження співбесіди;
- система надання правової допомоги в Україні;
- реєстрація в системі «Електронний суд»;
- алгоритм оформлення трудових правовідносин та ін.;

5) розроблення та розповсюдження інформаційних матеріалів (пам’яток) із правової тематики.

Економічний напрям, який реалізується шляхом:

1) проведення тренінгів для військовослужбовців та членів їх сімей із питань фінансово-економічної грамотності, що дозволить ефективно управляти своїми фінансовими ресурсами, планувати фінансові цілі та приймати незалежні рішення, дотримуватись розумних фінансових рішень, вибирати ефективні способи інвестування та досягнення фінансової стабільності й успіху в багатьох сферах життя;

2) проведення консультування з фінансової грамотності військовослужбовців та членів їх сімей;

3) залучення дітей військовослужбовців до роботи в наукових гуртках «Економіст» та «Сучасний бухгалтер»;

4) залучення військовослужбовців та членів їх сімей до обговорення питань відновлення держави «Молодь України як інтелектуальний потенціал нації».

Психологічний напрям, який передбачає системну психоедукацію (курси лекцій, практичних занять, вебінарів, майстер-класів, воркшопів) для військовослужбовців, членів сімей військовослужбовців, дітей військовослужбовців і практикуючих психологів щодо формування резильєнтності особистості та громади, надання першої психологічної допомоги та психологічного супроводу військовим, подолання наслідків посттравматичного синдрому та надання консультацій їх близьким родичам.

У межах реалізації цього напряму заплановано:

1) проведення вебінарів і майстер-класів за темами:

- «Харчова залежність: чому виникає та як її позбутися»;
- «Психологічна підтримка дітей в умовах воєнного стану»;
- «Воля як безцінний помічник у житті: кого можна назвати по-справжньому вольовим»;
- «Віковий та нейропсихологічний аспект регуляції поведінки у дітей»;
- «Травма та її наслідки»;
- «Резильєнтність сучасного фахівця в умовах сьогодення: засоби її формування, ефективні практики в роботі з дітьми»;
- «Емоційне вигорання: відновлення ресурсів»;
- «Принципи побудови емоційного, посередницького та регулятивного діалогу у взаєминах дітей і дорослих»;
- «Ресурси духовного здоров’я особистості у важких життєвих ситуаціях»;
- «Використання конструктора LEGO у роботі з агресивними дітьми»;
- «Психотерапія залежної поведінки»;
- «Техніки майндфулнес для саморегуляції стану в умовах стресу»;

- «Психологічний супровід переживання втрати»;
- «Емоційна пам’ять: звичайне функціонування й функціонування у важкі для людини часи»;
- «Благополуччя дітей і педагогів: дієві інструменти та практики психосоціальної підтримки»;
- «Особливості надання психологічної допомоги військовослужбовцям, ветеранам та членам їхніх сімей»;
- «Копінг-поведінка особистості в складних життєвих ситуаціях»;
- «Психоедукація сім’ї ветеранів: від травми війни до ресурсів її подолання»;
- «Техніки емоційного відновлення за програмою PIPA (програма професійного втручання у випадках переживання травматичних подій)»;

2) проведення психодіагностичної роботи з військовослужбовцями, членами сімей військовослужбовців на платформі Moodle – Методика: Шкала SCARED-P-дорослі (тривожні розлади та їх діагностика).

Логотерапевтична та психокорекційна допомога реалізується шляхом:

1) проведення діагностики особистості військовослужбовців та членів їх сімей;
2) розроблення програм логокорекційного та психокорекційного втручання, проведення психокорекційної роботи;
3) проведення індивідуально-групових психокорекційних і логокорекційних занять з військовослужбовцями, які мають розлади мовлення внаслідок нейротравм;
4) проведення індивідуального консультування військовослужбовців та членів їх сімей щодо розвитку та відновлення мовлення;
5) проведення вебінарів за такими темами:

- «Способи подолання труднощів ковтання у пацієнтів після інсульту»;
- «Комплексний підхід до подолання заїкання у дітей»;
- «Стимулювання процесу відновлення мовлення у пацієнтів з нейротравмами в умовах сім’ї»;
- «Надання первинної психологічної допомоги дітям з ментальними порушеннями в умовах війни»;
- «Завдання та напрями роботи з відновлення комунікативної функції мовлення у пацієнтів з афазією».

У межах діяльності Центру здійснюється *залучення військовослужбовців до проведення заходів з військового національно-патріотичного виховання* для здобувачів вищої освіти.

У межах реалізації цього напряму заплановано:

1) проведення загальноуніверситетських заходів, присвячених Міжнародному дню миру, Дню партизанської слави, Дню Захисників і Захисниць України, Дню Українського козацтва, Дню визволення України від фашистських загарбників, Дню Гідності і Свободи, Дню Збройних Сил України;
2) проведення зустрічей здобувачів вищої освіти з військовослужбовцями, присвячені Міжнародному дню миру, Дню партизанської слави, Дню Захисників і Захисниць України, Дню Українського козацтва, Дню визволення України від фашистських загарбників, Дню Гідності і Свободи, Дню Збройних Сил України;
3) проведення кураторських годин, під час яких здобувачі вищої освіти, чиї батьки є учасниками бойових дій, розповідатимуть на конкретних прикладах своїх родин, що мотивує українських захисників і захисниць на боротьбу за незалежність нашої держави, а також наскільки важливою для військових є повага та підтримка українського суспільства;
4) участь у конкурсі учнівських і студентських творів-есе з психології, присвяченому військовій та національно-патріотичній тематиці в межах програми VII Всеукраїнської науково-практичної конференції з міжнародною участю «Харківський осінній марафон психотехнологій»;
5) сприяння політиці національної пам'яті: пошанування загиблих, створення галерей і куточків пам'яті загиблих, дослідження біографій Героїв, збір свідчень у форматі усної історії про учасників бойових дій.

Для ефективної діяльності Центру ветеранського розвитку створена мультидисциплінарна команда, вектором діяльності якої є не тільки надання практичної допомоги, а і превенція негативних явищ. До складу мультидисциплінарної команди включені науково-педагогічні працівники та співробітники Харківського національного педагогічного університету імені Г. С. Сковороди, що дає можливість інтеграції якісних теоретичних знань у практичну діяльність. Також до роботи Центру залучені представники Юридичної клініки Харківського національного педагогічного університету імені Г. С. Сковороди, Психологічної служби Університету, стейкхолдери, які здійснюють практичну діяльність у відповідній сфері.

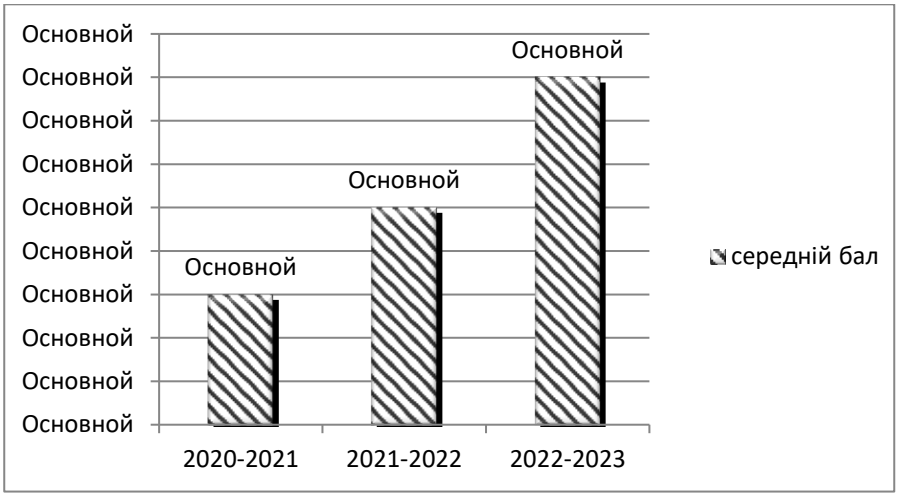
Для забезпечення діяльності та інформування про діяльність Центру створена сторінка на офіційному сайті Університету (http://hnpu.edu.ua/uk/division/centr-veteranskogo-rozvytku) та сторінка у Фейсбуці (https://www.facebook.com/groups/1015975216284486/?ref=share).

Діяльність Центру здійснюється на підставі відповідного плану роботи на 2023-2024 навчальний рік.

Неодмінним складником виховної системи вишу є функціонування газети «Учитель», на шпальтах якої відображаються найактуальніші подіх у виші, місті, країні, світі.

Виконання завдань зазначених напрямів виховання передбачає комплексне використання традиційних та інноваційних методів і форм виховання: індивідуально, в академічній групі (здійснюють куратор і викладач), у групах за інтересами (колективи художньої самодіяльності, спортивні секції, науково-проблемні групи, клуби за інтересами тощо).

Одним із критеріїв ефективності реалізації виховної системи Університету є рівень вихованості студентської молоді. У ЗВО для визначення рівня вихованості використовуємо опитувальник, розроблений відділом моніторингу, у якому представлені такі ціннісні орієнтири людини, як-от: любов до Батьківщини, ставлення до суспільства й держави, правова культура, національна ідентичність, культура поведінки, здоровий спосіб життя, дбайливе ставлення до природи, загальна ерудиція, ставлення до праці, до людей, до самого себе тощо. Процедура моніторингу рівня вихованості проводиться протягом декількох років (рис. 2.4).



2.4. Динаміка рівня вихованості здобувачів освіти

5 – 4,5 – високий рівень (в)

4,4 – 4 – достатній рівень (д)

3,9 – 2,9 – середній рівень (с)

2,8 – 2 – низький рівень (н)

Мета аналізу результатів моніторингу – вичленовування типових (для ЗВО й конкретних студентських груп) проблем, які можуть стати предметом управлінської роботи, управлінських розв'язків, насамперед методичного супроводу й підтримки професійного та особистісного зростання здобувачів в освітньому процесі.

Отже, проаналізувавши рівень розвитку виховної системи ЗВО, можна зробити висновок, що науково-педагогічний колектив працює над створенням життєтворчого

простору, у якому виховна система охоплює весь освітній процес, інтегруючи навчальні заняття, теоретичну та практичну підготовку студентів, позааудиторну діяльність здобувачів, різноманітну діяльність національно-патріотичного, громадського, професійного, соціального, природного, предметно-естетичного спрямування, яка безперервно розширюється й оновлюється.

Мікродослідження № 4. Оцінка стану моніторингу виховної діяльності ЗВО як управлінської проблеми.

Мета: здійснити оцінку стану моніторингу виховної діяльності закладу освіти як управлінської проблеми.

Задля виконання завдань дослідження ми розробили кваліметричну модель (табл. 2.2) оцінки стану моніторингу виховної діяльності як управлінської проблеми. Використання методів загальної кваліметрії як інструментарію моніторингу сприяє об'єктивному кількісному оцінюванню стану моніторингу як функції управління в закладі освіти. Факторно-критеріальне моделювання реалізує один із найголовніших принципів кваліметричного підходу: урахування взаємозв'язку між якостями як складних, так і простих властивостей предмета, що її визначають *(Г. Єльникова, 2004; З. Рябова, 2018)*.

Узагальнивши роботи В. Григораша, Г. Єльникової, З. Рябової, О. Касьянової, А. Єрмоли, Т. Хлєбнікової, В. Циби та інших, було визначено фактори, критерії та показники оцінки стану моніторингу виховної діяльності як управлінської проблеми.

Фактор (від лат. *factor* – той, що робить) розглядаємо як причину явища, що визначає його характер. Слово «критерій» «Словник іншомовних слів» визначає як ознаку, на підставі якої виробляється оцінка, визначення або основа для класифікації будь-чого.

Отже, спочатку визначили такі фактори:

- інформаційно-аналітичне забезпечення моніторингу виховної діяльності;
- планування моніторингу виховної діяльності;
- організація моніторингових досліджень з питань виховної діяльності;
- узагальнення результатів моніторингу виховної діяльності;
- контроль і корекція діяльності на основі результатів моніторингу виховної діяльності.

Далі визначили вагомість факторів та критеріїв за методом, запропонованим З. Рябовою, на засадах кваліметричного підходу.

До складу експертної групи ввійшло 17 осіб.

Визначення вагомості факторів проводили за 5-бальною оцінкою, оскільки факторів п'ять. Експерти визначали бали запропонованим факторам (табл. 2.1). Як видно із табл. 2.1, за першим фактором 6 експертів виставили 5 балів, 2 експерти – 4 бали, 2 експерти – 3 бали, 4

експерта – 2 бали, 3 експерта – 1 бал. Підраховуємо загальну кількість балів для першого фактору:

$\sum 1 = 6\times5 + 2\times4 + 2\times3 + 4\times2 + 3\times1 = 55.$

В аналогічний спосіб підраховуємо загальну кількість балів для факторів 2, 3 ,4, 5. Далі підраховуємо загальну кількість балів за всіма факторами:

$\sum = 55+50+54+46+46=251.$

Визначаємо вагомість (mi) кожного фактору таким чином: кількість балів за фактором ($\sum i$) треба розділити на загальну кількість балів ($\sum$):

$m1 = 55\div251= 0,22$; $m2 = 50\div251= 0,20$; $m3 = 54\div251= 0,22$; $m4 = 46\div251= 0,18$; $m5 = 46\div251= 0,18$.

Таблиця 2.1

Розрахунок вагомості факторів

Фактори	Бали					∑	mi
	5	4	3	2	1		
Фактор 1	6	2	2	4	3	55	0,22
Фактор 2	2	3	6	3	4	50	0,20
Фактор 3	7	1	3	3	3	54	0,22
Фактор 4	2	3	4	4	4	46	0,18
Фактор 5	-	8	3	3	2	46	0,18
Усього						249	1,0

У такий само спосіб розрахували вагомість критеріїв. Результатом роботи експертів стало впорядкування кваліметричної моделі оцінки стану моніторингу виховної діяльності як управлінської проблеми (табл. 2.2).

Оцінювання здійснювали, використовуючи шкалу від 0 до 1 з інтервалом у 0,25, від повної відсутності показника до повного його виявлення.

Обчислювання значення кожного фактору здійснювали за формулою:

$$Фi = mi\ (V1K1 + \ldots ViKi) \quad (2.1);$$

де **Ф** – фактор, **m** – вагомість фактору, **V** – вагомість критерію, **K** – усереднений коефіцієнт відповідності, **i** – порядковий номер.

Загальну оцінку стану моніторингу виховної діяльності визначали як суму всіх факторів.

Рівень здійснення моніторингу виховної діяльності ЗВО визначали за такою шкалою: $0 < O\ заг. \le 0,5$ – рівень критичний; $0,5 < O\ заг. \le 0,65$ – рівень недостатній; $0,65 < O\ заг. \le 0,7$ – рівень допустимий; $0,7 < O\ заг. \le 0,85$ – рівень достатній; $0,85 < O\ заг. \le 1$ – рівень високий.

Оцінку стану моніторингу виховної діяльності у ЗВО проводила група експертів із 5 осіб, до якої увійшли представники ректорату, факультетських керівників і Студентського парламенту.

Оцінка групи експертів представлена в таблиці 2.2 та на рис. 2.5, 2.6.

Таблиця 2.2

Кваліметрична модель
оцінки стану моніторингу виховної діяльності ЗВО
як управлінської проблеми

Фактори	**Вагомість**	**Критерії**	**Вагомість**	**Коеф. відп.**
1. Інформаційно-аналітичне забезпечення моніторингу виховної діяльності **$Ф_1=m_1(V_1K_1+V_2K_2+V_3K_3++V_4K_4)$**	$m_1=0,22$	1.Рівень обізнаності адміністрації та НПП, ПП з вимогами законодавчих, нормативних, інструктивних документів з питань виховної діяльності	$V_1=0,25$	К1=0,75
		2.Поінформованість керівників закладу про сутність і технологію моніторингу виховної діяльності	$V_2=0,25$	К2=0,75
		3.Поінформованість НПП, ПП закладу про сутність і технологію моніторингу виховної діяльності	$V_3=0,20$	К3=0,75
		4.Повнота аналізу роботи науково-педагогічного колективу з питань моніторингу виховної діяльності за минулий навчальний рік	$V_4=0,30$	К4=0,5
2. Планування моніторингу виховної діяльності закладу **$Ф_2=m_2 (V_5K_5+V_6K_6++V_7K_7+V_8K_8+V_9K_9)$**	$m_2=0,20$	5.Наявність в перспективному і річному планах роботи закладу розділу з питань моніторингу виховної діяльності закладу освіти	$V_5=0,20$	К5=0,75
		6.Координація планів роботи ЗВО з питань моніторингу виховної діяльності	$V_6=0,21$	К6=0,5
		7.Охоплення плануванням усіх напрямів роботи науково-педагогічного колективу щодо проведення моніторингу виховної діяльності	$V_7=0,3$	К7=0,75
		8.Конкретність планів і поставлених перед науково-педагогічним колективом	$V_8=0,16$	К8=0,5

		завдань із проведення моніторингу виховної діяльності		
		9.Призначення відповідальних за проведення моніторингових досліджень і узагальнення результатів	V_8=0,13	К9=0,75
3. Організація моніторингових досліджень результатів виховної діяльності закладу **$Ф_3=m_3(V_{10}K_{10}+V_{11}K_{11}+$** **$+V_{12}K_{12}+V_{13}K_{13}+V_{14}K_{14}+$** **$+V_{15}K_{15})$**	m_3=0,22	10.Розробка і затвердження програми моніторингу виховної діяльності	V_{10}=0,15	К10=0,5
		11.Розподіл обов'язків між адміністрацією, НПП і ПП, психологами щодо проведення моніторингових досліджень з проблем виховання	V_{11}=0,1	К11=0,5
		12.Готовність НПП, ПП до моніторингу виховної діяльності	V_{12}=0,25	К12=0,75
		13.Наявність відповідного інструментарію для проведення моніторингу виховної діяльності: кваліметричних моделей, методичних рекомендацій тощо	V_{13}=0,15	К13=0,75
		14.Чітке визначення термінів моніторингових досліджень	V_{14}=0,15	К14=0,75
		15.Інструктаж учасників моніторингу виховної діяльності	V_{15}=0,20	К15=0,5
4. Узагальнення результатів моніторингу виховної діяльності ЗВО **$Ф_4=m_4(V_{16}K_{16}+V_{17}K_{17}+$** **$+V_{18}K_{18}+V_{19}K_{19}+V_{20}K_{20})$**	m_4=0,18	16.Відбір і систематизація отриманої інформації щодо якості виховного процесу	V_{16}=0,20	К16=0,75
		17.Використання сучасних методів оброблення отриманих результатів моніторингу виховної діяльності	V_{17}=0,10	К17=0,75
		18.Своєчасність оброблення інформації	V_{18}=0,23	К18=0,5
		19.Достовірність і об'єктивність отриманих результатів моніторингу виховної діяльності	V_{19}=0,27	К19=0,75
		20.Гласність і повнота доведення до учасників ОП результатів моніторингу ВД	V_{20}=0,20	К20=0,75

5. Контролювання й корегування роботи за результатами моніторингу виховної діяльності ЗВО **$Ф_5=m_5(V_{21}K_{21}+V_{22}K_{22}+$** **$+V_{23}K_{23}+V_{24}K_{24})$**	m_5=0,18	21.Обговорення результатів моніторингу ВД на засіданнях Виконавчої ради	V_{21}=0,17	К21=0,75
		22.Обговорення результатів моніторингу ВД на засіданнях наукових рад факультетів	V_{22}=0,23	К22=0,75
		23.Внесення змін у процедуру моніторингу ВД на основі отриманих результатів	V_{23}=0,30	К23=0,5
		24.Коригування освітньої діяльності закладу загалом, структурних підрозділів та одиниць за результатами моніторингу ВД	V_{24}=0,30	К24=0,75

Розрахунки за кваліметричною моделлю розміщено в таблиці 2.3.

Таблиця 2.3

Обчислення за кваліметричною моделлю

№ з/п	Коефіцієнт відповідності критерію **Ki**	Вагомість критерію **Vi**	Оцінка критерію **ViKi**	**∑** критеріїв **Фi**	Вагомість фактору **mi**	Оцінка фактору **Фi**
1	К1=0,75 К2=0,75 К3=0,75 К4=0,75	0,25 0,25 0,20 0,30	0,1875 0,1875 0,15 0,225	0,425	0,22	**Ф1**=0,165
2	К5=0,75 К6=0,5 К7=0,75 К8=0,5 К9=0,75	0,20 0,21 0,30 0,16 0,13	0,15 0,105 0,225 0,08 0,0975	0,515	0,20	**Ф2**=0,1315
3	К10=0,5 К11=0,5 К12=0,75 К13=0,75 К14=0,75 К15=0,5	0,15 0,10 0,25 0,15 0,15 0,20	0,075 0,05 0,1875 0,1155 0,1125 0,1	0,5025	0,22	**Ф3**=0,14091
4	К16=0,75 К17=0,75 К18=0,5 К19=0,75 К20=0,75	0,20 0,10 0,23 0,27 0,20	0,15 0,075 0,115 0,2025 0,15	0,595	0,18	**Ф4**=0,124614
5	К21=0,75 К22=0,75 К23=0,5 К24=0,75	0,17 0,23 0,30 0,30	0,1175 0,1725 0,15 0,225	0,595	0,18	**Ф5**=0,1197
Загальна оцінка стану моніторингу ВД як управлінської проблеми				**О заг. = Ф1 + Ф2 + Ф3 + Ф4 +Ф5 = 0,681**		

Рівень стану моніторингу виховної діяльності в закладі освіти	**допустимий**

За шкалою визначаємо оцінку стану моніторингу виховної діяльності ЗВО як управлінської проблеми. Отже, коефіцієнт відповідності дорівнює 0,681, що відповідає допустимому рівню.

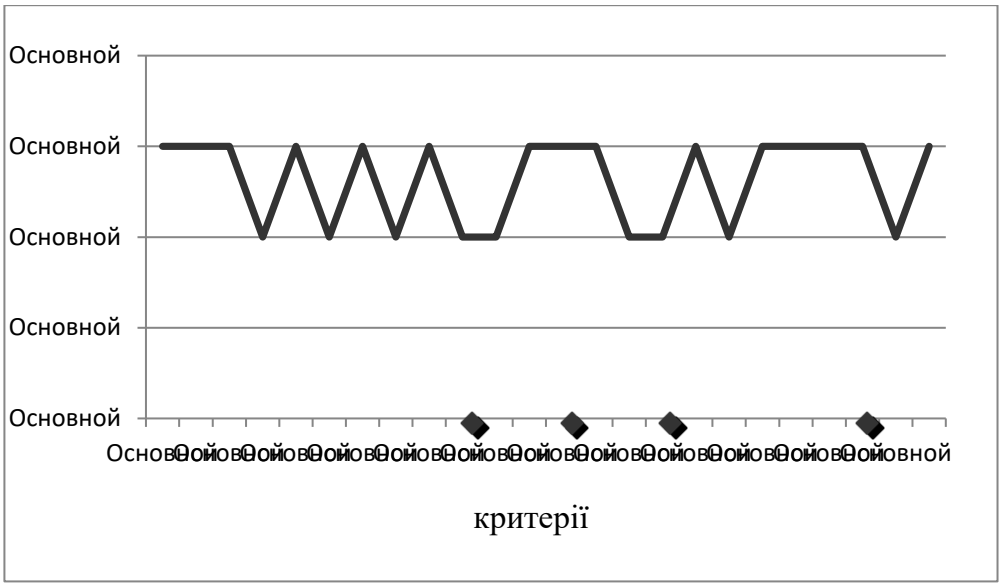


Рис. 2.5. Узагальнена експертна оцінка критеріїв за кваліметричною моделлю

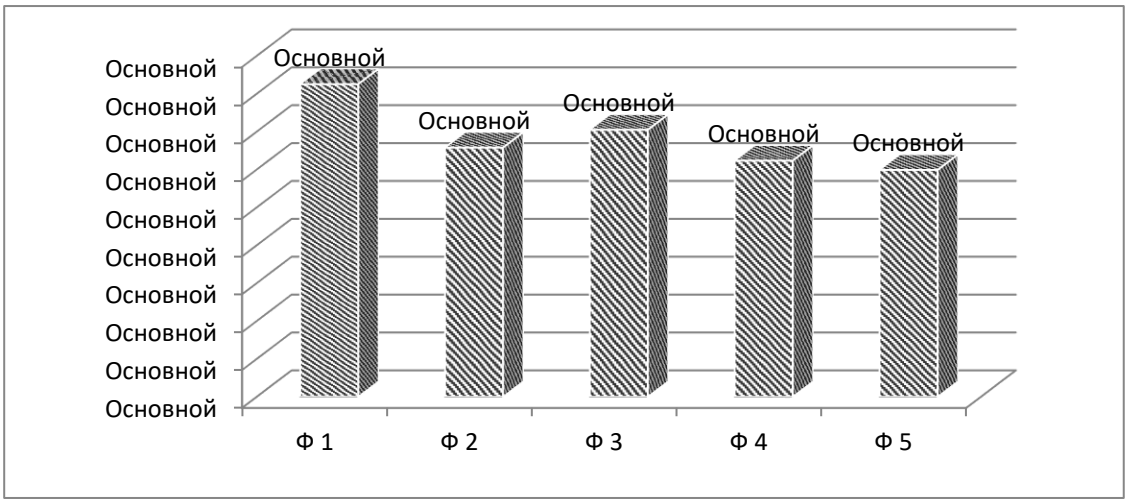


Рис. 2.6. Внесок кожного фактору з урахуванням вагомості

Отже, моніторинг виховної діяльності ЗВО як управлінська проблема потребує вдосконалення. У першу чергу слід покращити такі складники, як узагальнення результатів моніторингу ВД, контролювання й коригування роботи за результатами моніторингу ВД ЗВО. Вважаємо, що це доцільно буде зробити на основі програмно-цільового підходу, розробивши комплексно-цільову програму з удосконалення моніторингу ВД ЗВО як управлінської проблеми.

2.2. Комплексно-цільова програма з удосконалення моніторингу виховної діяльності вишу та її експертна оцінка

Проблема: відсутність систематичного відстеження результатів виховної діяльності, низька поінформованість керівника про якість виховання в закладі освіти, недостатній рівень моніторингу виховної діяльності ЗВО.

Загальна мета: створення оптимальних умов для впровадження моніторингу виховної діяльності в роботу закладу освіти та управлінську діяльність, підвищення якості моніторингу як функції управління та якості виховної діяльності ЗВО.

Цілі – напрями діяльності:

- визначити проблеми та вдосконалити інформаційно-аналітичну діяльність керівника з питань моніторингу виховної діяльності ЗВО;
- розробити та запровадити програму моніторингу результатів виховної діяльності ЗВО;
- урізноманітнити інструментарій моніторингу виховної діяльності шляхом створення факторно-критеріальних моделей оцінювання діяльності учасників ОП;
- підвищити якість стану моніторингових досліджень результатів виховної діяльності у закладі освіти;
- координація видів і напрямів діяльності закладу освіти щодо надання якісних освітніх послуг.

Концептуальні ідеї:

- кваліметричний підхід до розроблення факторно-критеріальних моделей оцінки діяльності;
- моделювання та розроблення програми моніторингу результатів виховної діяльності;
- упровадження розробленої програми моніторингових досліджень результатів виховної діяльності;
- перетворення кількісних показників у якісні;
- прогнозування рівня вихованості студентів, рівня розвитку студентського колективу і колективів студентських груп, превентивний характер управлінських рішень, забезпечення інформаційної стабільності для прийняття управлінських рішень щодо якості виховної діяльності.

Термін упровадження: 1,5 року (серпень 2024 – грудень 2025 рр.)

План реалізації заходів

Етап	Мета	Напрямок та завдання	Очікувані результати	Термін
Підготовчий	Здійснення проблемно-орієнтованого аналізу діяльності	1.Розробка, обговорення, корекція методологічних засад і технології	Наявність технології здійснення моніторингу	Серпень, вересень 2024р.

	факультетів щодо впровадження моніторингу виховної діяльності для формування банку даних за його результатами, корекція управлінської діяльності, прогнозування розвитку закладу освіти.	здійснення моніторингу виховної діяльності ЗВО. 2.Опитування щодо основних напрямків управлінської діяльності керівників факультетів із упровадження моніторингу якості виховання. 3.Підготовка пакету документів для проведення самомоніторингу та моніторингу виховної діяльності закладу. 4.Навчання НПП, ПП організації та проведення моніторингу виховної діяльності. 5.Розроблення програмно-методичного забезпечення впровадження моніторингу ВД ЗВО. 6.Створення технології оброблення	виховної діяльності ЗВО. Виокремлення досвіду управління з упровадження моніторингу виховної діяльності та недоліків у роботі керівників для подальшої корекційної роботи. Пакет документів для проведення самомоніторингу та моніторингу виховання. Оволодіння НПП, ПП інноваційними технологіями оцінювання та набуття знань, умінь, навичок щодо впровадження моніторингу виховної діяльності. Наявність усіх програм, методичних розробок для впровадження моніторингу ВД ЗВО. Наявність технології	Вересень, жовтень 2024р. Жовтень 2024р. Протягом року Протягом року Жовтень 2024р.

		результатів моніторингу. 7.Забезпечення мотиваційної готовності здобувачів освіти до впровадження моніторингу виховної діяльності. 8.Підвищення рівня управлінської компетентності керівників щодо впровадження моніторингу результатів виховної діяльності	оброблення результатів моніторингу. Поінформованість студентів щодо мети, змісту моніторингу виховання. Високий рівень управлінської компетентності керівника щодо впровадження моніторингу виховної діяльності	Протягом року Протягом року
Практичний	Ефективна реалізація моніторингу виховної діяльності ЗВО	1.Теоретичні семінари з НПП, ПП щодо впровадження моніторингу результатів виховної діяльності 2.Вивчення емоційної рівноваги, моральних якостей НПП, ПП, кураторів, керівників структурних підрозділів, задіяних у ВД. 3.Проведення психологічних тренінгів із розвитку психолого-педагогічної	Доведення до відома, обговорення з НПП, ПП основ діяльності закладу освіти щодо ефективного впровадження моніторингу виховної діяльності. Високий рівень емоційної рівноваги, високі моральні якості. Розвиток професійної компетентності НПП, ПП	Жовтень 2024 р. Протягом року Листопад 2024 - квітень 2025 р.р.

		компетентності кураторів, професійної компетентності НПП, ПП.		
		4.Проведення діагностичних вимірювань, тестів, анкетувань студентів, НПП, ПП із проблем виховної діяльності.	Визначення якості виховання, розвитку виховної системи ЗВО, виховних систем студ. груп, рівнів вихованості здобувачів.	Квітень, травень 2025р
		5.Проведення опитування студентів щодо якості освітніх послуг у закладі освіти.	Визначення думки студентів щодо задоволення рівнем виховної діяльності.	Травень 2025 р.
		6.Проведення експертизи розроблених програм, моделей для проведення моніторингу виховної діяльності.	Визначення найкращих розробок.	Серпень 2025р.
		7. Розроблення у ЗВО програми підвищення ефективності впровадження моніторингу виховання.	Розроблення комплексно-цільової програми з урахуванням ресурсного забезпечення ЗВО.	Червень - серпень 2025р.
		8.Підготовка та проведення Виконавчої ради з питань результативності впровадження моніторингу виховної діяльності	Визначення ефективності процесу впровадження моніторингу виховної діяльності ЗВО	Вересень 2025р.
Корекційний	Внесення необхідних корективу у	1.Відстеження конкретних прогалин у рівні	Оптимізація проведення моніторингу.	Жовтень 2024-травень 2025 р.р.

	методологічну основу проведення моніторингу виховної діяльності ЗВО.	розвитку виховної системи, вихованості здобувачів, виявлення причин, що впливають на якість виховання. 2.Організація корекційної роботи. 3.Проведення засідань вчених рад факультетів, обмін досвідом	 Накопичення та обмін досвідом з роботи над проблемою. Систематизація накопиченого досвіду	 Жовтень 2024-травень 2025 р.р. Протягом терміну реалізації програми
Підсумковий	Визначення результативності впровадження моніторингу ВД ЗВО	1.Створення робочої групи з узагальнення результатів роботи з впровадження моніторингу виховання, порівняння показників з минулими роками. 2. Визначення рівня вихованості студентів. 3. Визначення рівня професійної компетентності НПП, ПП закладу. 4. Визначення перспектив і напрямів подальшої роботи ЗВО щодо використання моніторингу якості виховної діяльності. 5.Проведення науково-практичної конференції	Створення робочої групи та визначення плану її роботи. Узагальнення результатів. Узагальнення даних дослідження. Складання перспективного плану, плану розвитку діяльності з упровадження моніторингу ВД. Систематизація накопиченого матеріалу.	Серпень 2025р. Вересень 2025р. Листопад 2025р. Грудень 2025р Грудень 2025 р.

		«Моніторинг ВД: напрями і перспективи розвитку»	Видання навч.-метод. альманаху.	

Перед затвердженням програми Вченою радою університету вона була направлена на експертизу спеціалістам. До складу експертної комісії ввійшли заступники деканів із виховної роботи.

Експерти оцінювали розроблену комплексно-цільову програму за критеріями і показниками, представленими в Додатку А. Оцінки експертів представлено в таблиці 2.4 та на рис. 2.7, 2.8.

Таблиця 2.4

Прогнозована якість комплексно-цільової програми

Критерії експертизи	Е 1	Е 2	Е 3	Е 4	Е 5	Ki
Кр 1	1	1	1	0,88	0,77	0,93
Кр 2	1	0,88	1	1	0,88	0,9
Кр 3	0,77	1	0,88	0,88	1	0,91
Кр 4	0,88	0,88	1	0,88	0,88	0,93
Кр 5	1	0,88	1	1	0,88	0,95
Кр 6	0,83	0,91	1	0,91	0,91	0,92
Кр 7	1	1	1	1	0,83	0,97
Кр 8	1	1	0,66	1	0,83	0,9
Кр 9	1	1	0,88	1	1	0,98
Заг. оцінка	0,954	0,967	0,92	0,954	0,923	0,93

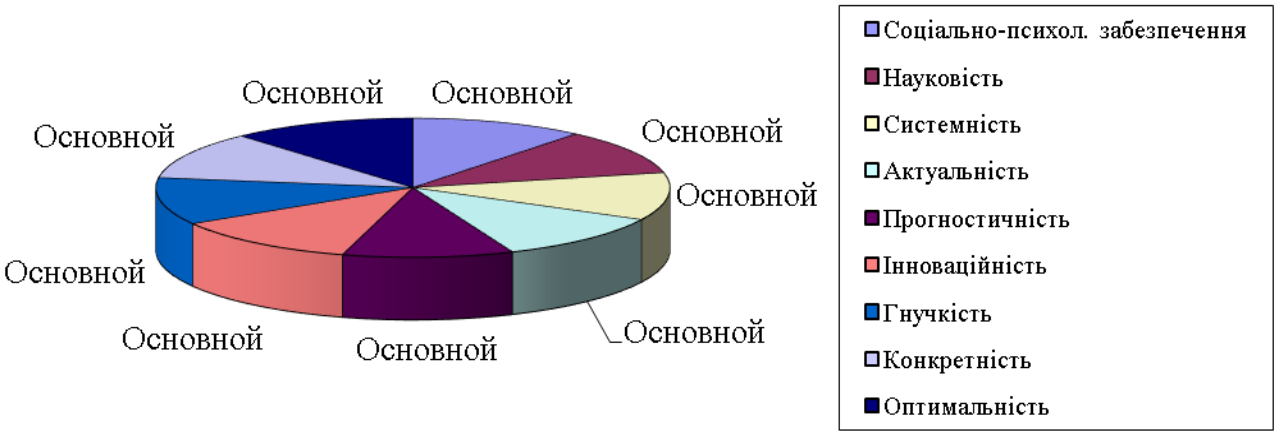


Рис. 2.7. Внесок кожного коефіцієнта в загальну суму Ki

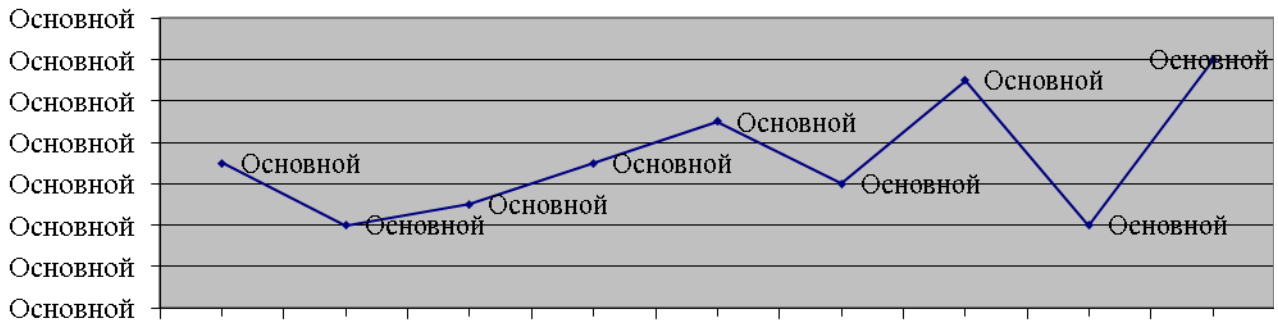


Рис. 2.8. Загальна оцінка кожного критерію програми

Як видно із таблиці 2.7, загальна експертна оцінка комплексно-цільової програми дорівнює 0,93, що відповідає **достатньому** рівню. Тому ця програма була рекомендована експертною групою для впровадження в роботу ХНПУ імені Г. С. Сковороди.

Реалізацією програми управляє творча група.

Для ефективного впровадження комплексно-цільової програми необхідно створити належні умови, а саме:

1) організаційно-педагогічні:

- визначення чітких цілей і завдань моніторингу ВД;
- своєчасне коригування планів роботи, повідомлення виконавців;
- контролювання проведення передбачених планом заходів;
- прийняття рішень за результатами контролю: усунення відхилень, стимулювання НПП, ПП, студентів до активної діяльності; аналіз проведеного, інформування керівництва ЗВО;
- оптимальне навчальне навантаження, громадські доручення, рівномірне завантаження учасників ОП;
- проведення хронометражу робочого часу учасників експерименту, установлення непродуктивних витрат та їх усунення;
- спеціалізація й кооперація управлінської та педагогічної праці – раціональний розподіл доручень, визначення схем і складання циклограм діяльності, за рахунок чого економиться час;
- створення опорних кабінетів, пунктів, методичного центру для надання допомоги у реалізації програми;

2) морально-психологічні:

- стимулювання НПП, ПП до реалізації запланованих заходів;

- розроблення й упровадження системи морального та матеріального забезпечення учасників експерименту;
- розвиток мотиваційної сфери НПП, ПП;
- надання учасникам експерименту пільг, облік результативності їхньої роботи, зарахування цих активностей до рейтингу;

3) матеріально-технічні:

- розроблення фінансово-економічного забезпечення реалізації програми, кошторису валових витрат, визначення статей фінансових надходжень, залучення спонсорів до фінансування проекту;
- обладнання ЗВО інформаційними приладами, науково-методичною літературою для здійснення запланованих заходів;
- упровадження автоматизованої системи інформаційного забезпечення управління;
- створення з дотриманням правил безпеки кабінету психологічного розвантаження, використання його можливостей для проведення тренінгових занять, групових та індивідуальних консультацій, релаксаційної гімнастики тощо;

4) санітарно-гігієнічні:

- організація умов для повноцінного харчування;
- організація спортивно-оздоровчої роботи з НПП, ПП та колективом здобувачів освіти;
- дотримання температурного, повітряного, світлового режимів у процесі виконання програми.

Нами проведено експертну оцінку умов, створених у ЗВО для реалізації розробленої програми.

Експертна оцінка умов для впровадження комплексно-цільової програми

Мета: оцінити наявність умов, які сприяють результативності впровадження комплексно-цільової програми в практику роботи ЗВО.

Відповідно до мети дослідження, нами було розроблено протокол оцінки створених у закладі освіти умов для впровадження комплексно-цільової програми, за допомогою якого було здійснено аналіз відповідних умов у ХНПУ імені Г. С. Сковороди (додаток Б).

Результати експертної оцінки (узагальнені дані) занесені до табл. ДБ і графічно представлені на рис. 2.9.

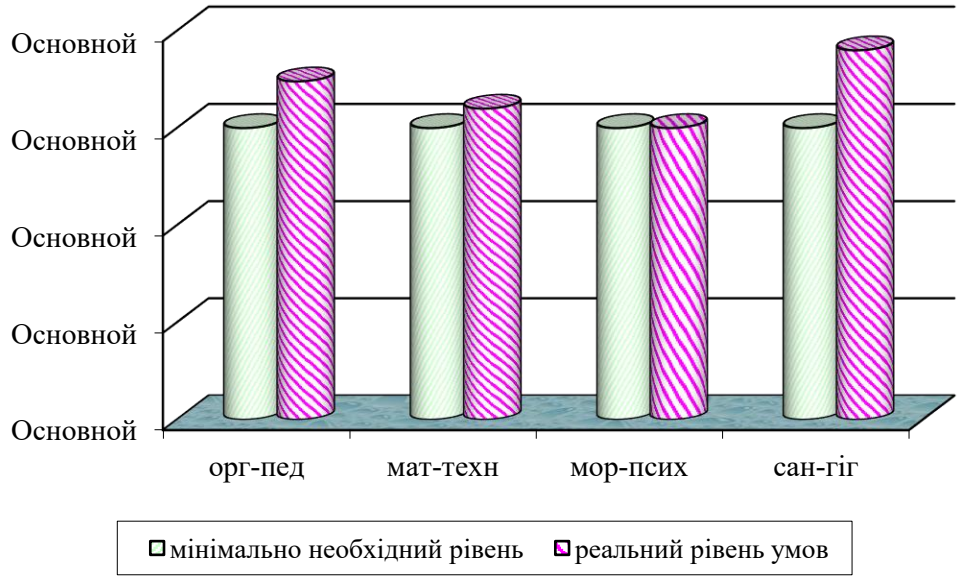


Рис. 2.9. Експертна оцінка умов для реалізації КЦП

Отже, оцінка умов, створених для впровадження КЦП з удосконалення моніторингу виховної діяльності вишу, дорівнює **0,84**, що відповідає **достатньому рівню**. Адміністрації ЗВО необхідно врахувати недоліки, виявлені експертною групою, спрямувати роботу щодо їх усунення й оптимізації зовнішніх та внутрішніх умов.

Для успішної реалізації КЦП пропонуємо дотримувати таких рекомендацій:

1) моніторинг як функцію управління, у тому числі моніторинг виховної діяльності, удосконалювати на основі програмно-цільового підходу, ураховуючи принципи системності, актуальності, прогностичності, раціональності, реалістичності, цілісності, контрольованості, науковості, послідовності та об’єктивності;
2) узгодити впровадження розробленої й затвердженої КЦП із стратегією розвитку ЗВО, річним планом роботи та загальною програмою впровадження моніторингу в діяльність ЗВО;
3) створити картотеку з питань перспективного педагогічного досвіду щодо проблеми освітнього моніторингу;
4) забезпечити надходження систематичної оперативної інформації про нові методичні рекомендації, публікації стосовно проблеми моніторингових досліджень в освіті;
5) створити з числа НПП творчу групу в складі 4–6 осіб, яка буде брати участь у розробленні стандартизованих моделей моніторингу, у підготовці й проведенні моніторингових процедур;
6) підбирати виконавців програми відповідно до їх функціональних обов’язків та особистих можливостей;
7) основними завданнями творчої групу можуть бути такі:

- організація і проведення діагностики учасників ОП з метою визначення їхньої думки стосовно якості освітніх послуг у закладі освіти, зокрема, якості виховної діяльності;
- створення банку інформації стосовно питань освітнього моніторингу;
- розроблення й реалізація психолого-педагогічних проектів з метою підвищення рівня професійної компетентності кураторів і рівня вихованості студентів, рівня розвитку студентських груп і загалом колективу вишу;
- проведення соціологічних досліджень із упровадження моніторингових досліджень;

8) утілити в практику роботи ЗВО систематичне діагностування психологічного клімату педагогічного колективу з метою корекції відхилень та створення оптимальних умов для продуктивності ОП;
9) поширювати виступи НПП, ПП із питань проведення моніторингових досліджень на засіданнях вчених рад факультетів, засіданнях кафедр, науково-практичних семінарах, конференціях;
10) подальше вдосконалення кваліметричної моделі оцінки моніторингу виховної діяльності на основі виокремлення «проблемних зон»;
11) регулярне інформування НПП, ПП і студентів про результати комплексного оцінювання за кваліметричною моделлю (не менше одного разу на півріччя);
12) дотримання принципів гласності, демократизму: дані моніторингових досліджень не повинні стати підставою для покарання НПП чи ПП. Вони є підґрунтям для своєчасного внесення коректив в діяльність творчої групи, у систему роботи НПП і ПП, керівників гуртків і секцій, систему роботи адміністративної ланки.

ВИСНОВКИ

Теоретико-прикладні пошуки та проведена робота дають підстави дійти таких висновків. На основі аналізу наукової літератури було визначено особливості виховної діяльності ЗВО й управління нею на сучасному етапі. Так, необхідно протистояти викликам сьогодення, таким як військова агресія рф, низький рівень розвитку навичок спілкування, перманентний стрес, доступність молоді до руйнівного контенту, знецінення соціальних зв’язків, брак часу на реалізацію виховних проектів через онлайновий формат освіти або перенавантаження студентів.

Особливостями виховної діяльності у ЗВО насамперед є спрямованість виховання на професійний розвиток, професійне становлення майбутнього фахівця, розвиток його національної ідентичності та морально-психологічних якостей.

Основна мета моніторингу полягає у виявленні спроможності установи освіти (зокрема виховної системи ЗВО) сприяти розвитку особистості здобувача. Це виявляється в

забезпеченні ефективного інформаційного відбиття стану виховання у вищій школі, аналітичному узагальненні результатів діяльності, розробленні прогнозу розвитку виховної системи ЗВО.

Особливістю моніторингу виховної діяльності ЗВО є багатоаспектність напрямів виховної діяльності, значна кількість учасників виховної діяльності, відсутність стандартів вихованості.

Розроблення системи моніторингу виховної діяльності ЗВО припускає два основні етапи: аналітико-прогностичний і організаційно-технологічний.

Мета моніторингу виховної діяльності – виявити потенційний ресурс виховання й розробити стратегію його реалізації.

До основних інструментів моніторингу виховання відносимо кваліметричні моделі, засобами моніторингу є спостереження, опитування різного роду, оброблення статистичної інформації, експертна думка тощо.

Для результативності моніторингу виховної діяльності необхідно дотримувати алгоритму, описаного вище. Задля вдосконалення моніторингу виховної діяльності слід дотримувати принципів системності, об'єктивності, цілісності, науковості, послідовності тощо.

Упровадження теоретико-методологічних засад вдосконалення моніторингових досліджень виховної діяльності було апробовано в ХНПУ імені Г. С. Сковороди. Зокрема, було визначено готовність педагогічних і науково-педагогічних працівників до впровадження моніторингових досліджень. За допомогою діагностичних методик проведено ґрунтовний аналіз якості виховання студентів, а саме: виявлено рівень вихованості здобувачів вищої освіти, проведено аналіз кадрового забезпечення освітніх програм, аналіз напрямів виховної діяльності університету.

Було проаналізовано стан моніторингу відповідно до мети дослідження, за результатами якого встановлено, що рівень управлінської діяльності з упровадження моніторингу виховної діяльності вишу недостатній. Відтак задля вдосконалення управлінської діяльності за означеним напрямом було розроблено КЦП, проведено її експертну оцінку, надано методичні рекомендації щодо її впровадження. Програма розрахована на півтора роки, отримала схвальну оцінку експертної групи, рекомендована Вченою радою до впровадження. Реалізація комплексно-цільової програми передбачає створення в закладі освіти відповідних умов: організаційно-педагогічних, морально-психологічних, матеріально-технічних, санітарно-гігієнічних тощо.

Отже, поставлену мету досягнуто, завдання виконано. Однак проведене дослідження не є вичерпним, тому перспективами в цьому напрямі ми вважаємо подальше розроблення факторно-критеріальних моделей для визначення якості роботи ЗВО.

References:

Бень В. В. (2019). Проблема національної самоідентичності серед українського студентства: *Матеріали XIII Всеукраїнської студентської наукової конф. Умань:* ВПЦ «Візаві», 2019. С. 12–16.

Блохіна І. (2023). До проблеми професійної підготовки майбутніх фахівців з управління навчальними закладами в сучасних умовах. *Актуальні питання у сучасній науці.* 2023. № 11 (17). С. 766–777. URL: http://perspectives.pp.ua/index.php/sn/article/view/7355/7397.

Бурдонос Л., Виноградня В., Вераксіч С. (2023). Діджиталізація та сучасне інформаційне забезпечення менеджменту персоналу. *Актуальні питання у сучасній науці.* 2023. № 11 (17). С. 60–70. DOI: https://doi.org/10.52058/2786-6300-2023-11(17)-60-70.

Виноградова Т. І. (2016). Патріотичне виховання студентів як багатокомпонентний процес. *Теорія і методика виховання.* Херсон, 2016. № 6. С. 13–16.

Виноградський М. Д. (1998). Менеджмент організацій. Київ : КНЕУ, 1998.

Гречаник О. Є., Борисенко Н. О. (2023). Актуальні проблеми менеджменту виховної діяльності. *Наукові перспективи. Сер. : Економіка.* 2023. № 1 (31). С. 272–297. DOI: 10.52058/2708-7530-2023-1(31)-258-27.

Гречаник О. Є., Борисенко Н. О. (2023). Маркетингові комунікації як засіб підвищення якості діяльності закладу освіти. *Використання технологій менеджменту якості в управлінні закладами освіти:* зб. мат-лів ІІ Всеукр. наук.-практ. конф. (м. Тернопіль, Україна, 17 листопада 2023 року) / Ред. : І. М. Вітенко, Р. С. Брик, Н. Р. Бабовал, О. В. Городецька, Т. Г. Дідух. Тернопіль, 2023. 224 с.

Гречаник О. Є., Грабар О. В. (2021). Професійне навчання як засіб розвитку корпоративної культури персоналу організації. *The Scientific Heritage*. 2021. No 81. VOL. 3. P. 29-32.

Гречаник О. Є., Григораш В. В. (2019). Організація внутрішнього аудиту в закладі загальної середньої освіти. Харків, 2019. 144 с.

Гречаник О. Є. (2020). Оцінка якості виховної діяльності закладу загальної середньої освіти. *Адаптивне управління: теорія і практика. Сер. : Педагогіка.* Харків : УІПА, 2020. Вип. 8 (15). URL: https://doi.org/10.33296/2707-0255-8(15)-12.

Гречаник О.Є., Хлєбнікова Т. М., Темченко О. В. (2022). Digital-маркетинг як інструмент антикризового розвитку підприємств. *Економіка та суспільство*. 2022. № 43. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1767.

Григораш В. В. (2014). Маркетингова діяльність директора школи. Харків : Основа, 2014. 144 с.

Григораш В. В. (2011). Організація діяльності керівника школи. Харків : Основа, 2011. 224 с.

Григораш О. В. (2020). Акмеологічна оцінка управлінської культури керівника закладу освіти. *Освіта дорослих: світові тенденції, українські реалії та перспективи :* колект. моногр. Харків : ХНПУ, 2020. С. 255-260.

Дудка І. А. (2015). Патріотичне виховання студентської молоді як складова громадської діяльності вищого навчального закладу. *Витоки педагогічної майстерності. Сер. : Педагогічні науки.* 2015. № 16. С. 56–63.

Єльникова Г. В. (2017). Адаптивні технології в освіті. *Адаптивне управління: теорія і практика. Серія «Педагогіка».* 2017. Вип. 3 (5). URL: http://am.eor.in.ua/images/adapt/Vol.3ped5/17ped3_5yelnikova_r.pdf.

Єльникова Г. В. (2004). Основи адаптивного управління. Харків : Основа, 2004.

Зеліч В. В., Євтухова С. М., Гречаник О. Є. (2021). Аналіз показників комунікативного менеджменту підприємства при здійсненні маркетингового аудиту. *Наукові перспективи. Серія : Економіка.* 2021. № 9 (15). С. 286-297.
Золотухіна С. Т., Зеленська Л. Д. (2007). Професійно-педагогічна компетентність викладача вищого навчального закладу (історико-педагогічний аспект). Харків : ХНПУ, 2007. 185 с.
Ішутіна О. Є. (2018). Проблема моніторингу якості вищої освіти в Україні. *Science Review.* 2018. № 5 (12). Vol. 1. DOI: https://doi.org/10.31435/rsglobal_sr/01062018/5624.
Каленюк І. С. (2003). Економіка освіти. Київ : Знання, 2003. 40 с.
Кіндрат І. Р. (2013). Управлінські аспекти моніторингу якості дошкільної освіти в умовах інтегрованого освітнього процесу. *Modern directions of theoretical and applied researches.* 2013. № 19–30 March. URL: http://www.sworld.com.ua/index.php/ru/conference/the-content-of-conferences/archives-of-individual-conferences/march-2013.
Козак Л. В. (2018). Педагогічний моніторинг як технологія управління якістю дошкільної освіти. *Педагогічна освіта: теорія і практика. Психологія. Педагогіка : зб. наук. пр.* 2018. № 30. С. 40–45. URL: https://pedosvita.kubg.edu.ua/index.php/journal/article/view/203/295.
Концепція національно-патріотичного виховання в системі освіти України. URL: https://nus.org.ua/wp-content/uploads/2022/06/62a0421e24258666156501.pdf.
Кульчицький В. Й. (2021). До питання моніторингу патріотичного виховання школярів. *Вісник Університету імені Альфреда Нобеля. Сер. : Педагогіка і психологія.* 2021. № 1 (21). С. 33–37.
Лозова В. І., Троцко А. В. (2002). Теоретичні основи виховання і навчання: Навч. посіб. Харків : ОВС, 2002. 400 с.
Мармаза О. І. (2016). Інноваційний менеджмент. Харків : ХНПУ, 2016. 197 с.
Мармаза О. І. (2003). Організаційна культура управління. *Управління школою*. 2003. № 7.
Мармаза О. І. (2015). Стратегічний менеджмент. Харків : ТОВ «Планета-Прінт», 2015. 103 с.
Мартинюк В. (2023). Модель формування національної ідентичності студентської молоді в закладах вищої педагогічної освіти у поза аудиторній роботі. *Актуальні питання у сучасній науці.* 2023. № 11 (17). С. 958–970. URL : http://perspectives.pp.ua/index.php/sn/article/view/7371/7413.
Мастеркова Т. (2018). Розвиток професійної компетентності педагога в міжатестаційний період на засадах адаптивного управління. *Адаптивне управління: теорія і практика. Сер. : Педагогіка.* 2018. Вип. 5 (9). URL: https://amtp.org.ua/index.php/journal/article/view/107/74 (дата звернення: 27.02.2020).
Міхеєв В. І. (2010). Моделювання і методи теорії вимірів в педагогіці. Київ, 2010. 224 с.
Нижник Н., Пашко Л. (2005). Управлінська культура: теоретичне поняття чи управлінська поведінка? Політичний менеджмент. 2005. № 5. С. 103-113. URL: https://ipiend.gov.ua/wp-content/uploads/2018/07/nyzhnyk_upravlinska.pdf.
Олійник Л. (2022). Безпечна школа: виклики системи освіти в умовах війни. 2022. URL : https://jurfem.com.ua/bezpechna-shkola-vyklyky-systemy-osvity-v-umovakh-viyny (дата звернення : 15.09.2023).
Організація безпечного освітнього середовища – виклик сучасності: перспективи та рішення. *Науковий, методичний, інформаційний збірник Тернопільського обласного комунального інституту післядипломної педагогічної освіти* / Ред. : О. М. Петровський, В. С. Мисик, І. М. Вітенко та ін. Тернопіль : ТОКІППО, 2023. 416 с.
Попова О. В., Денисенко А. О., Васильєва С. О. (2021). Моніторинг якості освіти в сучасних ЗВО. *Теорія та методика навчання та виховання.* 2021. № 51. С. 133–145. DOI: 10.34142/23128046.2021.51.13.
Репко І. П. (2015). Педагогічні основи національно-патріотичного виховання студентської молоді. *Наукові записки кафедри педагогіки.* Харків, 2015. № 38. С. 10–19.
Рожнова Т. (2023). Вплив управління закладом професійно-технічної освіти на засадах інноваційних технологій на професійну підготовку кваліфікованих робітників. *Актуальні*

питання у сучасній науці. 2023. № 10 (16). С. 714–729. URL: http://perspectives.pp.ua/index.php/sn/article/view/6812/6849.
Рябова З. В. (2018). Кваліметричний підхід до оцінювання якості надання освітніх послуг. *Адаптивне управління: теорія і практика. Серія «Педагогіка».* 2018. Вип. 5 (9). URL: https://amtp.org.ua/index.php/journal/article/view/107/74.
Савчук Л., Бурлакова А. (2005). Розвиток корпоративної культури в Україні. *Персонал.* 2005. № 5. URL: http://personal.in.ua/article.php?ida=68.
Сисоєва С. О. (2000). Проблема формування особистості, здатної до творчої самореалізації. *Наукові праці. Т. 7. Серія : Педагогіка.* 2000. С. 13–19.
Темченко О. В. (2019). Теоретичні аспекти моделювання в системі управління якістю освіти. *Забезпечення якості освіти: підходи, моделі, механізми реалізації* / За заг. ред. Т. М. Хлєбнікової. Харків : ХНПУ ; «Мірта», 2019. С. 27-38.
Темченко О. В. (2010). Педагогічні умови формування професійної позиції вчителя загальноосвітньої школи : автореф. дис.… на здобуття наук. ступеня канд. пед. наук : спец. 13.00.04. Харків : ХНПУ, 2010. 22 с.
Темченко О. В. (2019). Теоретичні аспекти моделювання в системі управління якістю освіти. *Забезпечення якості освіти: підходи, моделі, механізми реалізації* / За заг. ред. Т. М. Хлєбнікової. Харків : ХНПУ ; «Мірта», 2019. С. 27-38.
Ткаченко В. (2023). Забезпечення ефективності освітньої діяльності університетів в умовах воєнного стану та післявоєнного відновлення: управлінські технології. *Актуальні питання у сучасній науці.* 2023. № 11 (17). С. 1034–1042. URL : http://perspectives.pp.ua/index.php/sn/article/view/7378/7420.
Фадєєв В. І., Ганжа С. М., Ганжа С. А. (2009). Маркетинг освітніх послуг. Євпаторія : Кримський Афон, 2009. 168 с.
Харківська А. (2014). Сутність педагогічного моніторингу якості виховного процесу у вищих педагогічних навчальних закладах. 2014. URL : http://repository.khpa.edu.ua:8080/jspui/bitstream/123456789/2569/1/4F4C~1.PDF.
Хлєбнікова Т. М., Гречаник О. Є., Григораш В. В. (2018). Акмеологічний супровід педагога в процесі саморозвитку. *Scientific Educational Center RS Global Sp. Z. O.O. Science Review*. 2018. № 6 (13), July.
Хміль Ф. І. (2006). Управління персоналом. Київ : Академвидав, 2006.
Шостак Л. В., Болодан Є. О. (2018). Зарубіжний досвід управління персоналом. *Приазовський економічний вісник.* 2018. Вип. 3 (08). URL: http://inneco.org/article/view.
Ягупов В.В., Свистун В. І., Кришталь М. А., Король В. М. (2013). Управлінська культура і компетентність керівників як системна психолого-педагогічна проблема. *Збірник наукових праць Національної академії державної прикордонної служби України. Серія : «Педагогічні та психологічні науки».* 2013. № 4 (96). С. 291-301.
Яременко С. (2023). Стратегічні комунікації в управлінні. *Актуальні питання в сучасній науці.* 2023. № 11 (17). С. 485–495. URL : https://doi.org/10.52058/2786-6300-2023-11(17)-485-495.
Becker B. E., Huselid M. A., Ulrich S. D. (2001). The HR Scorecard. Linking People, Strategy and Performance. Boston : Harvard Business School Press, 2001.
Covey S. R. (2004). The 7 habits of highly effective people: Restoring the Character Ethic. New York, Free Press, 2004.
Grygorash V., Grechanyk O. (2020). Forming acmeological competence of potential education managers. *Theory and Practice of Future Teacher's Training for Work in New Ukrainian School*: monograph / Edit. I. F. Prokopenko, I. M. Trubavina. Prague, 2020. P. 102-112.
Klebnikova T. (2020). Personally-oriented approach to the formation of the new ukrainian school teacher. *Theory and Practice of Future Teacher's Training for Work in New Ukrainian School:* monograph (колективна монографія). Prague, OKTAN PRINT s.r.o., 2020. P. 133-155.
Powell M. (2016). Human resource management practices in Japan. *Merici.* 2016. Vol. 2. Pp. 77-90.

Tusheva V., Vasylieva S., Agarkova N., Grygorash V., Grechanyk O. (2020). The phenomenon of a future tearcher's scientific-research culture under the new socio-cultural conditions. *Journal of Critical Reviews.* 2020. Vol. 7. Issue 13. URL: https://drive.google.com/file/d/1pBFrJ-FuVcc-6Sm8_Lpd50DT_bbchEa6/view.

ДОДАТКИ

Додаток А

Таблиця ДА

Протокол експертизи комплексно-цільової програми

№	Критерії	Показники	Оцінки експертів					Кі
			Е1	Е2	Е3	Е4	Е5	
1.	***Актуальність***	1.Відповідність вимогам сучасності.	3	3	3	3	3	1,00
		2.Детермінація соціально-педагогічних умов функціонування закладу.	3	3	3	3	2	0,93
		3.Зорієнтованість на вирішення пріоритетних проблем управління, які впливають на результативність діяльності закладу	3	3	3	2	2	0,87
	Загальна оцінка за критерієм 1		9	9	9	8	7	**0,93**
2.	Науковість	4.Використання досягнень психолого-педагогічної науки, теорії та практики управління ЗВО.	3	3	3	3	3	1,00
		5.Відображення суттєвого змісту проблеми.	3	2	3	3	2	0,93
		6.Передбачення використання діагностичних методів при реалізації програми.	3	3	3	3	3	1,00
	Загальна оцінка за критерієм 2		9	8	9	9	8	**0,9**
3.	Конкретність та можливість реалізації на кожному етапі	7.Враховуються особливості та можливості ЗВО.	3	3	3	2	3	0,93
		8.Передбачені конкретні управлінські дії, заходи.	2	3	2	3	3	0,87
		9.Визначена мета, термін, зміст діяльності кожного етапу	2	3	3	3	3	0,93
	Загальна оцінка за критерієм 3		7	9	8	8	9	**0,91**
4.	Системність	10.Простежується система у вивченні проблеми.	3	3	3	3	3	1,00
		11.Наявність моделі організаційних зв’язків у колективі та її дієвість.	2	2	3	3	2	0,87
		12.Всі дії та заходи підпорядковані кінцевій меті	3	3	3	2	3	0,93
	Загальна оцінка за критерієм 4		8	8	9	8	8	**0,93**
5	Оптимальність	13.Ефективне використання часу, коштів, кадрів.	3	3	3	3	3	1,00
		14.Неприпустимість перевантаження й непотрібних пауз.	3	2	3	3	3	0,93

		15.Можливість використання іншими ЗВО	3	3	3	3	2	0,93
	Загальна оцінка за критерієм 5		9	8	9	9	8	**0,95**
6	Соціально-психологічне забезпечення	16.Прогностичність напрямків розвитку психологічної служби закладу.	2	3	3	3	3	0,93
		17.Наявність соціально-психологічних методів управління.	2	3	3	2	3	0,87
		18.Можливість передбачення результатів впливу на колектив ЗВО.	3	2	3	3	2	0,87
		19.Створення умов для саморозвитку особистості студента, НПП та ПП	3	3	3	3	3	1,00
	Загальна оцінка за критерієм 6		10	11	12	11	11	**0,92**
7	Інноваційність	20.Ступінь новизни в діяльності керівника.	3	3	3	3	2	0,93
		21.Ступінь новизни в діяльності НПП, ПП.	3	3	3	3	3	1,00
	Загальна оцінка за критерієм 7		6	6	6	6	5	**0,97**
8	Прогностич-ність	22.Можливість розв'язання проблем управління, які ще не виявлені.	3	3	2	3	3	0,93
		23.Передбачення можливих вимог до управління освітою	3	3	2	3	2	0,87
	Загальна оцінка за критерієм 8		6	6	4	6	5	**0,9**
9	Гнучкість	24.Відкритість, припустимість удосконалення.	3	3	3	3	3	1,00
		25.Можливість контролю, регулювання та корекції.	3	3	3	3	3	1,00
		26.Наявність механізмів самовдосконалення.	3	3	2	3	3	0,93
	Загальна оцінка за критерієм 9		9	9	8	9	9	**0,98**

Технологія оцінювання. Експертні оцінки виставляються за кожним показником залежно від ступеня його реалізації: 0 балів – показник відсутній; 1 бал – показник недостатньо виражений; 2 бали – показник достатньо виражений; 3 бали – показник оптимально виражений.

Якщо ступінь реалізації показника залежить тільки від його наявності, то твердженню «так» відповідає оцінка 3 бали, твердженню «ні» — 0 балів.

Загальна експертна оцінка кожного критерію була обчислена за формулою:

$$\mathbf{K = n / N,\ K \leq 1,}$$

де **n** – сума балів, виставлених експертами, **N** – максимальна кількість балів.

Загальна експертна оцінка всієї програми обчислювалася за формулою:

$$K = (1/9) \left(\sum_{i=1} K_i \right), (K < 1),$$

де **K** – показник загального рівня програми, **Ki** – показник реалізації кожного окремого критерію, **i** = 1, 2, 3...9.

Відповідно до отриманих результатів експертною групою було визначено рівень програми на етапі планування згідно зі шкалою:

$0 \leq K \leq 0,5$ – рівень незадовільний;

$0,5 < K \leq 0,65$ – рівень критичний;

$0,65 < K \leq 0,8$ – рівень допустимий;

$0,8 < K \leq 0,95$ – рівень достатній;

$0,95 < K \leq 1$ – рівень оптимальний.

Додаток Б

Таблиця ДБ

Протокол експертизи умов, створених у закладі освіти для впровадження комплексно-цільової програми з удосконалення моніторингу виховної діяльності ЗВО

Умови	***Критерії***	***Експ. оцінка***
1.Організаційно-педагогічні	1. Наявність чіткої системи роботи з НПП, ПП з питань упровадження моніторингу виховної діяльності у ЗВО.	5
	2. Оптимальний розподіл часу на проведення запланованих заходів, урахування навчального навантаження НПП.	4
	3. Забезпеченість керівників структурних підрозділів та НПП кваліметричними моделями оцінки параметрів і показників.	5
	4. Організація самоосвітньої діяльності НПП, спрямованої на підвищення рівня обізнаності з проблем моніторингових досліджень.	4
	5. Використання персоналізованого підходу при впровадженні моніторингу як управлінської функції.	4

	6. Забезпечення наступності навчання і виховання на різних рівнях вищої освіти.	4
Загальна оцінка організаційно-педагогічних умов		***0,87***
2.Матеріально-технічні	1. Науково-методичне забезпечення Університету для виховання і розвитку студентів, у т.ч. віртуальне освітнє середовище.	4
	2. Наявність та робочий стан ТЗН, можливість їх використання з метою саморозвитку особистості студента й НПП, реалізації запланованих заходів тощо.	3
	3. Забезпеченість наукової бібліотеки літературою з питань впровадження моніторингу виховної діяльності.	4
	4. Забезпеченість факультетів, кафедр відповідною літературою з означеної проблеми.	4
	5. Оформлення офіційного сайту ЗВО та представлення на ньому відповідних матеріалів.	5
Загальна оцінка матеріально-технічних умов		***0,8***
3.Морально-психологічні	1. Розробленість системи морального та матеріального стимулювання НПП, ПП до проведення моніторингових процедур.	3
	2. Наявність системи психологічної роботи з керівниками структурних підрозділів із підвищення якості системи моніторингових досліджень у ЗВО.	4
	3. Наявність системи психологічної роботи з НПП, ПП із розвитку їхньої готовності до проведення моніторингових досліджень.	4
	4. Сформованість професійно-педагогічної компетентності НПП, ПП.	4
Загальна оцінка морально-психологічних умов		***0,75***
4.Санітарно-гігієнічні	1. Організація харчування учасників експерименту.	5
	2. Наявність кабінетів психологічного розвантаження.	
	3. Організація спортивно-оздоровчої роботи з НПП, ПП, студентами.	5
	4. Забезпечення температурного, світлового, повітряного режиму для роботи з упровадження КЦП.	5
		4
Загальна оцінка санітарно-гігієнічних умов		***0,95***
Загальна оцінка створених у закладі умов		***0,84***

Додаток В

Узагальнені дані анкетування кураторів студентських груп щодо знань і вмінь у сфері виховання

№	*Зміст роботи куратора*	*Самооцінка кураторів*	*Оцінка адміністрації*
І. Вивчення соціально-педагогічних умов діяльності куратора студентської групи			
1.	Вивчення культури поведінки здобувачів освіти	2,6	2,3
2.	Вивчення запитів, нахилів, інтересів здобувачів освіти	1,8	1,2
3.	Педагогічний аналіз контингенту здобувачів освіти, які потребують особливої уваги	2	2,3
4.	Вивчення рівня вихованості здобувачів освіти	1,4	1,2
5.	Вивчення рівня розвитку студентських груп	2,8	2,6
6.	Аналіз та діагностика професійної діяльності	2,4	1,8
7.	Забезпечення співпраці з іншими учасниками освітнього процесу	2	1,7
Середній бал		***2,14***	***1,87***
ІІ. Планування та розроблення основних напрямів роботи			
1.	Планування роботи куратора	2,5	2,4
2.	Планування виховних заходів зі студентською групою, у тому числі в онлайн форматі	2,6	2,3
3.	Планування індивідуальної роботи зі здобувачами освіти	2,3	2,1
4.	Планування роботи з науково-педагогічними працівниками, які викладають освітні компоненти в групі	3	2,8
Середній бал		***2,6***	***2,4***
ІІІ. Організація роботи зі студентською групою			
1.	Організація роботи з реалізації завдань та основних напрямків національно-патріотичного виховання	2,4	2,1
2.	Розвиток творчих здібностей здобувачів освіти, залучення їх до різноманітних видів діяльності, у тому числі в онлайн форматі	2,2	1,7
3.	Організація морально-правового виховання	2,3	2,1
4.	Організація роботи студентського самоврядування	2,5	2,2
5.	Проведення виховних заходів зі студентською групою	2,5	2,1
6.	Організація роботи зі здобувачами освіти, які потребують особливих умов навчання, виховання й розвитку	2,2	2,1
Середній бал		***2,35***	***2,05***
IV. Робота з представниками місцевого самоврядування, громадськими організаціями			
1.	Організація та проведення волонтерської діяльності	1,8	1,9
2.	Організація взаємодії з іншими структурними підрозділами Університету, які здійснюють виховну діяльність (газета «Учитель», спортклуб, музейний комплекс)	2,3	2,2

3.	Залучення здобувачів освіти до роботи в культурно-мистецькому центрі	2	1,8
4.	Організація спільної діяльності з громадськими організаціями та рухами	1,6	1,4
5.	Залучення студентів до проведення профорієнтаційних заходів	2,4	2,0
Середній бал		***2,02***	***1,86***

Додаток Д

Оцінка якості виховної діяльності закладу освіти

Фактори	Вагомість фактору	Критерії	Вагомість критерію	Оцінка критерію	Ступ. відп. критерію	Ступ. відп. фактору
1. Якість особистісного розвитку вихованців	0,3	Ціннісне ставлення особистості до суспільства й держави (патріотизм, національна свідомість, політична та правова культура, готовність працювати задля розквіту держави, захищати її, поважати право, свободу, демократію)	0,09			
		Ціннісне ставлення особистості до людей (єдність моральної свідомості та поведінки, єдність слова і діла, наявність активної за формою та моральної за змістом життєвої позиції, чесність, чуйність, толерантність, уміння працювати в команді, інтелігентність, гуманізм тощо)	0,11			
		Ціннісне ставлення особистості до себе (почуття власної гідності, розвиток самості, суб’єктності, свідоме ставлення до життєвого вибору)	0,08			
		Ціннісне ставлення особистості до природи (усвідомлення цінності природи, відповідальність за неї, екологічно безпечна поведінка, природоохоронні навички)	0,07			
		Ціннісне ставлення особистості до мистецтва (шанобливе ставлення до творів мистецтва, естетичні почуття та смаки, ерудиція, культура сприйняття)	0,08			
		Ціннісне ставлення особистості до праці (потреба в трудовій активності, працелюбність, наявність професійних інтересів, конкурентоспроможність, підприємливість)	0,08			
		Ціннісне ставлення до родини, матері, сімейних цінностей	0,09			
		Ціннісне ставлення до здоров’я (свого, інших людей)	0,1			
		Адаптивність, мобільність	0,08			
		Креативність, ініціативність	0,07			
		Протистояння проявам несправедливості й жорстокості, цькування, булінгу	0,06			

		Мовна культура, уміння говорити, слухати, взаємодіяти	0,09			
2. Якість розвитку учнівського колективу	0,2	Наявність спільної мети, інтересів, цінностей	0,17			
		Перспективи в соціально-важливій діяльності	0,12			
		Згуртованість, узгодженість у роботі, взаємодопомога, дружба, товариськість	0,15			
		Наявність та ефективність самоврядування	0,14			
		Дієвість громадської думки	0,1			
		Дисципліна та взаємовимогливість	0,09			
		Прагнення до спілкування у вільний час	0,11			
		Творче самовираження особистості	0,12			
3. Якість професійної діяльності педагогів як вихователів	0,23	Професійні знання, науково-теоретична підготовка (знання нормативно-правової бази з питань виховної діяльності, психолого-педагогічних засад виховної діяльності, сучасних підходів до виховання)	0,17			
		Професійні вміння (володіння методикою виховної роботи, планування, організування діяльності (кожного вихованця, класного колективу, батьківського колективу), контролювання, коригування, аналізування результатів діяльності, педагогічна просвіта)	0,24			
		Професійно-особистісні якості (любов і повага до людей, довіра, доброта, щирість, гуманність, креативність, фасилітаторська позиція, доброзичливість, віра, креативність, мобільність, ініціативність)	0,15			
		Соціальна взаємодія та партнерство (співпраця з батьками – індивідуальні, групові, колективні форми роботи, колегами, громадськими об’єднаннями)	0,11			
		Самовдосконалення, громадська позиція (ставлення до професії, самоосвіта, підвищення кваліфікації, розповсюдження досвіду (публікації, виступи, майстер-класи і т. ін.), наставництво, консультування, класне керівництво, керівництво гуртками, УО, членство в ГО, пов’язаних із професійною діяльністю)	0,1			
		Позитивне ставлення до педагога з боку вихованців, їх батьків, колег, адміністрації ЗЗСО	0,12			

		Виконання посадових обов'язків (дотримання посадової інструкції, етичного кодексу ЗЗСО, трудова дисципліна, ведення ділової документації)	0,11			
4. Якість виховного середовища, умов забезпечення виховної діяльності	0,27	Організаційно-педагогічні (виховна система ЗЗСО, виховні системи класних колективів, система виховної роботи з розвитку здобувачів освіти, корпоративна культура й етичний кодекс ЗЗСО)	0,2			
		Морально-психологічні (позитивний соціально-психологічний клімат, мотивація, система стимулювання, особиста підтримка керівників, партисипативний стиль управління, партнерство, спільні цінності)	0,19			
		Кадрові (забезпечення педагогами, відсутність вакансій, відповідність посадовим і кваліфікаційним вимогам)	0,17			
		Інформаційні (Інтернет-ресурси, веб-сайт ЗЗСО, забезпечення періодичнми, методичними, фаховими виданнями з проблем виховання, доступність і якість інформаційно-бібліотечного центру)	0,15			
		Науково-методичні (наявність програми, проекту, концепції виховної діяльності, програм і планів роботи органів учнівського самоврядування, гуртків, учнівських об'єднань, методичні розробки, рекомендації, узагальнення ППД)	0,16			
		Матеріально-технічні (спортивна зала, актова зала, спортивний майданчик, облаштованість території для дітей із особливими потребами, обладнання й облаштування кабінетів і території для реалізації завдань виховної діяльності)	0,13			

DOI 10.5281/zenodo.10820391
UDC 341.232(477):061.1(100)

CHAPTER 4.

INTERNATIONAL ORGANIZATIONS AS A SUBJECT OF FORMATION, MAINTENANCE AND STRENGTHENING OF THE WORLD LEGAL ORDER AND SECURITY

Olha DZHYHORA,
PhD in Economics, Associate Professor,
Associate Professor of the Department of National Security, Public Management and Administration, Zhytomyr Polytechnic State University,
(103 Chudnivska St., Zhytomyr, Ukraine),
kebpua_dom@ztu.edu.ua,
https://orcid.org/0000-0001-8490-3917

Abstract. The article defines the essence of the concepts of "world order" and "security" in the context of globalization. The role and significance of international organizations as voluntary associations of states with specific goals in maintaining international peace and security are characterized. The factors contributing to the formation of international organizations are investigated. The functions and distinctive features of the main international organizations in the field of security are considered, with the main focus on the United Nations (UN), the European Union (EU), the Council of Europe (CoE), the Organization for Security and Cooperation in Europe (OSCE), and the North Atlantic Treaty Organization (NATO). The author identifies the areas of activity of international organizations in the sector of formation, maintenance and strengthening of world order and security. The world map of the Conflict Index rating and the rating of the levels of violent conflicts in the world are analyzed. The importance of streamlining relations between sovereign states, modernizing multilateral institutions and creating an effective oversight body to strengthen the global security system is emphasized. The main tasks of the UN Security Council in maintaining world order and security in the modern world are identified. The effectiveness of the UN Security Council in the context of the Russian-Ukrainian war is assessed. The study advocates the development of new international legal norms, including various aspects of international cooperation and strengthening of international institutional structures to combat new global challenges.

Keywords: international organization, world order, security, conflict index, UN Security Council, NATO, EU, OSCE, peacekeeping operations, Russian-Ukrainian war.

МІЖНАРОДНІ ОРГАНІЗАЦІЇ ЯК СУБ'ЄКТ ФОРМУВАННЯ, ЗАБЕЗПЕЧЕННЯ ТА ЗМІЦНЕННЯ СВІТОВОГО ПРАВОПОРЯДКУ ТА БЕЗПЕКИ

Анотація. Визначено сутність понять «світовий правопорядок» і «безпека» в контексті глобалізації. Охарактеризовано роль та значення міжнародних організацій як добровільних об'єднань держав з конкретними цілями у підтриманні міжнародного миру та безпеки. Досліджено фактори, що сприяють утворенню міжнародних організацій. Розглянуто функції та відмінні риси основних міжнародних організацій у сфері забезпечення безпеки, з основним акцентом на Організацію Об'єднаних Націй (ООН), Європейський Союз (ЄС), Раду Європи (РЄ), Організацію з безпеки і співробітництва в Європі (ОБСЄ), Організацію Північноатлантичного договору (НАТО). Визначено напрями діяльності міжнародних організацій у секторі формування, забезпечення та зміцнення світового правопорядку та безпеки. Проаналізовано світову карту рейтингу індексу конфліктності та рейтинг рівнів насильницьких конфліктів у світі. Підкреслено важливість впорядкування відносин між суверенними державами, модернізації багатосторонніх інституцій та створення ефективного наглядового органу для зміцнення глобальної системи безпеки. Визначено основні завдання Ради Безпеки ООН у підтримці світового правопорядку та безпеки в сучасному світі. Оцінено ефективність діяльності Ради Безпеки ООН у рамках російсько-української війни. Дослідження виступає за розробку нових міжнародних правових норм, включаючи різні аспекти міжнародного співробітництва та зміцнення міжнародних інституційних структур для боротьби з новими глобальними викликами.

Ключові слова: міжнародна організація, світовий правопорядок, безпека, індекс конфліктності, Рада Безпеки ООН, НАТО, ЄС, ОБСЄ, миротворчі операції, російсько-українська війна.

Вступ. Проблема визначення ролі та значення міжнародних організацій у підтриманні міжнародного миру та безпеки незмінно перебувають у центрі уваги вітчизняних і зарубіжних науковців. В останні роки в різних дослідженнях проаналізовано багато питань, пов'язаних з функціонуванням міжнародних організацій, серед яких: нормативні основи світового порядку (ООН та інші міжнародні організації); реформа ООН та її вплив на сучасну систему міжнародних відносин; проблема розбіжностей у розумінні сутності зусиль ООН у сфері підтримання міжнародного миру та безпеки; протиріччя моделі колективної безпеки. З моменту створення

Організації Об'єднаних Націй у 1945 році цілі підтримання міжнародного миру і безпеки шляхом запобігання конфліктам і надання допомоги сторонам конфлікту в примиренні завжди були і є основоположними в її діяльності. Основними формами та напрямками діяльності ООН з підтримання миру та безпеки є превентивна дипломатія та посередництво; миротворча діяльність; розбудова миру; боротьба з тероризмом; роззброєння.

Основна відповідальність за підтримання міжнародного миру і безпеки належить Раді Безпеки ООН, яка у свою чергу відіграє провідну роль у визначенні наявності загрози миру або акту агресії. Від імені Ради Безпеки до сторін, що сперечаються, звертаються із закликами до мирного врегулювання конфлікту, а також вносяться пропозиції щодо шляхів та умов врегулювання. Рада Безпеки має повноваження застосовувати примусові заходи для підтримання або відновлення міжнародного миру і безпеки відповідно до Глави VII Статуту ООН. Економічні санкції на міжнародні військові дії є прикладами таких дій. Рада Безпеки ООН також створює миротворчі операції ООН та спеціальні політичні місії. Незважаючи на те, що міжнародне співтовариство через механізми ООН вимагає від держав захисту населення від геноциду, воєнних злочинів, етнічних «чисток» і злочинів проти людяності, відповідальність держав у цій сфері часто зводиться до політичного, а не юридичного рішення.

Війна в Україні, розв'язана російською федерацією, яка за своєю жорстокістю перевершила Другу світову війну і триває вже понад два роки, продемонструвала неспроможність існуючих механізмів підтримання миру та миротворчості. ООН у цьому військовому конфлікті займає позицію стороннього спостерігача і коментатора, не маючи ефективних механізмів позитивного втручання. Можливі миротворчі операції (місії) стримуються фактом неминучої резонансної політизації миротворчої операції в цьому конфлікті та дисбалансом інтересів ключових учасників ООН, а також економічними (переважно енергетичними) чинниками. Таким чином, миротворча система виявилася не готовою до реальних і гібридних до реальних і гібридних викликів і загроз.

Постановка проблеми. Питання забезпечення міжнародної безпеки, набули особливого значення та актуальності на рубежі 90-х років XX століття у зв'язку з розпадом біполярної системи міжнародних відносин, що базувалася на політиці балансу сил у забезпеченні міжнародного миру та формуванні нового світового порядку. Саме в цей період пріоритетним став «широкий» підхід до визначення міжнародної безпеки та політики її забезпечення, що передбачає збалансовану увагу до різних вимірів міжнародної безпеки - військового, економічного, політичного, інформаційного, екологічного, особистісного та соціального. Такий підхід до забезпечення міжнародної безпеки сьогодні може стати ефективним підґрунтям для функціонування міжнародних політичних інституцій у сфері

безпеки: Організації Об'єднаних Націй, Ради Європи, Організації з безпеки і співробітництва в Європі, Європейського Союзу та Північноатлантичного альянсу. Однак реалізація широкого підходу до безпеки вимагає повномасштабного реформування основних міжнародних політичних інститутів, які є спадщиною холодної війни і, у зв'язку з цим, зберігають більшою чи меншою мірою традиційні структури і підходи до реалізації безпекової політики.

Аналіз останніх досліджень і публікацій. Аналізу діяльності міжнародних організацій присвятили свою увагу багато зарубіжних та вітчизняних науковців: Н. Бехруз, Ю. Битяк, Ф. Вільямс, Р. Горсон, М. Грушко, Х. Гужва, А. Гуляєв, І. Козловський, В. Ковалевський, Л. Ринейська, Д. Ронфельд, К. Стерлінг, В. Шемшученко, А. Шміда та інші. Незважаючи на широкий спектр наукових досліджень у сфері безпеки, у сучасній науці не приділялася належна увага дослідженню ролі та значення, а також ефективності діяльності міжнародних організацій у секторі забезпечення міжнародного правопорядку та безпеки.

У сфері міжнародного миру та безпеки сьогодні працюють багато установ системи ООН, а також регіональні міжнародні організації, неурядові інституції та громадські ініціативи. Оскільки Рада Безпеки ООН поступово розширює перелік «загроз міжнародному миру та безпеці», проблема розвитку взаємодії між міжнародними урядовими та неурядовими організаціями задля зміцнення міжнародного миру стає все більш актуальною.

Серед інституцій, залучених до зміцнення міжнародного миру і безпеки, варто виокремити регіональні, універсальні спеціалізовані інституції та неурядові неприбуткові організації. Серед міжнародних організацій повноваженнями з підтримання миру і безпеки наділені: Організація з безпеки і співробітництва в Європі (ОБСЄ), Європейський Союз (ЄС), Асоціація держав Східної Азії (АСЕАН), Організація Договору про колективну безпеку (ОДКБ).

Питання міжнародного миру та безпеки інтегровані в мандат універсальних спеціалізованих організацій (як тих, що входять до системи ООН, так і незалежних), таких як ЮНЕСКО, ЮНІСЕФ, ВООЗ, ПРООН, Інтерпол тощо. Особливу роль і функцію в питаннях підтримання міжнародного миру і безпеки виконують міжнародні суди - Міжнародний кримінальний суд (МКС), а також так звані «гібридні» трибунали, створені в рамках процесів примирення.

Перспективи еволюції світового порядку в багатьох аспектах визначатимуться спроможностями міжнародних організацій (держав-учасниць і секретаріатів), їх здатністю адаптуватися самим та адаптувати систему міжнародних відносин, міжнародне право до змін, що відбуваються. Від цього залежатиме їх привабливість для потенційних членів і партнерів, їх міжнародний авторитет, легітимність та ефективність.

1. Роль та значення міжнародних організацій у формуванні та підтримці світового правопорядку і глобальної безпеки

Міжнародне співробітництво створює умови для участі держави в розв'язанні спільних проблем і надає додаткові можливості для вирішення власних. Для країн, що розвиваються, таке співробітництво є не лише засобом зміцнення власних позицій на міжнародній арені, більш вагомого впливу на регіональні і глобальні процеси, але й джерелом компенсації браку національних ресурсів (фінансових, економічних, політичних), потрібних для реалізації внутрішньої і зовнішньої політики. Водночас, держава бере на себе додаткові зобов'язання та повинна бути готова до можливих ризиків і нових викликів, пов'язаних з їх виконанням чи невиконанням з різних причин (політичних, ресурсних, організаційних).

Міжнародні організації створюються і функціонують для вирішення проблем, які виходять за межі однієї держави. Вони відіграють вирішальну роль у забезпеченні світового порядку та глобальної безпеки. Слід підкреслити, що сьогодні питання забезпечення міжнародної та національної безпеки є одними з пріоритетних і мають суттєве значення для діяльності кожної держави. Вони також є предметом вивчення, наукових досліджень, уваги громадянського суспільства та внутрішньополітичної боротьби.

Міжнародні організації відіграють важливу роль у керівництві та реформування сфери безпеки. Вони надають інформацію та консультації; підвищують поінформованість з питань безпеки; фінансують навчання, програми та проекти з багатьох важливих питань, таких, як технічні навички, керівництво сектором безпеки, нагляд, розбудова доброчесності. Міжнародні організації також відіграють провідну роль у процесі нормотворчості, забезпеченні підзвітності та верховенства права. Крім того, вони забезпечують канал зв'язку між урядами та суспільством, а також між різними країнами, іншими міжнародними органами та діячами, що займаються керівництвом та реформуванням сфери безпеки.

Участь міжнародних організацій у реформуванні сфери безпеки почала збільшуватися у 1990-х рр., коли вони усвідомили, що заходи розвитку, особливо під час і після конфліктів, не можуть бути успішними в умовах загроз. Керівництво сферою безпеки почали розглядати як важливий елемент організації, врядування і проектів реконструкції. Крім того, демократичний нагляд за сферою безпеки став важливою умовою партнерських відносин і членства в таких організаціях, як ЄС, НАТО і Рада Європи.

Відтоді участь міжнародних організацій у процесах реформування сфери безпеки перетворилась на лавину заходів і проектів, що перетинаються між собою. Це особливо стосується країн під час та після конфліктів, де різні міжнародні організації змагаються за донорів і матеріально-людські ресурси. Співпраця та координація міжнародних організацій та

інших діячів, залучених до реформування сектору безпеки, надважливі для успіху програм демократичного врядування і, зрештою, впровадження ефективного демократичного урядування сферою безпеки.

Переважна більшість міжнародних організацій працюють у відносно обмежених і самостійних сферах (фінансовій, економічній, безпековій, гуманітарній, екологічній тощо), не вимагають єдності ціннісних засад, форм, способів урядування своїх членів і не торкаються найбільш суперечливого питання – державного суверенітету. З метою підвищення своєї легітимності та ефективності в розв'язанні нагальних проблем, вони зацікавлені в якомога більшій кількості членів, не вирішуючи за них питань орієнтирів розвитку. Водночас, одним із головних завдань інтеграційних утворень є визначення перспектив розвитку організації та її членів, які добровільно погодилися на передачу частини суверенітету наднаціональним органам, наділивши їх відповідними повноваженнями (9).

Питання міжнародного правопорядку та впливу на нього міжнародних організацій систематично досліджуються в науковій доктрині. Неоднозначність у розумінні дослідниками поняття «міжнародний правопорядок» зумовлює необхідність подальшого дослідження цієї категорії. Перш за все, слід розглянути базову категорію «правопорядок». Незважаючи на її широке використання в національних нормативно-правових актах, вона досі не має офіційного визначення. Згідно з Великим тлумачним словником сучасної української мови, «правопорядок» визначається як суспільний порядок, урегульований нормами права (2).

У теоретико-правовій науці відсутній єдиний підхід щодо визначення поняття міжнародного правопорядку. Оскільки міжнародне право формується на договірних засадах та принципах, то суб'єктами міжнародного правопорядку виступають учасники цих договірних зобов'язань, що несуть відповідальність за їх недотримання та невиконання (3).

Поняття «світовий порядок» доцільно розглядати як стан системи міжнародних відносин, належним чином запрограмований на її безпеку, стабільність і розвиток та регульований на основі критеріїв, що відповідають поточним потребам.

Порядок відносин між суверенними національним державами доцільно визначити як ядро сучасного міжнародного правопорядку. Обов'язковими елементами правопорядку повинні бути міжнародно-правові відносини та норми, що врегульовують та впорядковують такі відносини.

В основі міжнародного правопорядку містяться наступні положення: затверджені та погоджені міжнародним співтовариством права та основні свободи людини і громадянина, а також інші правила, що регулюють стосунки між суб'єктами міжнародного співтовариства (зокрема, державами) і прийняті, у вигляді звичаїв або багатосторонніх міжнародних угод;

стандарти, що встановлені двосторонніми або багатосторонніми угодами, що регулюють взаємодію між державами, або принципи врегулювання суперечок, що виникають між ними; норми міжнародного права, що регулюють стосунки між державами і іншими суб'єктами, що становлять міжнародне співтовариство, як в мирний час, так і під час війни (5).

З огляду на різні тлумачення поняття «міжнародний правопорядок», доцільно виділити три ключові елементи, які формують міжнародний правопорядок як окрему правову категорію:

1) міжнародні правовідносини;

2) міжнародні правові норми;

3) міжнародна законність (2).

Реальний характер міжнародного правопорядку забезпечується існуванням і функціонуванням глобальних і регіональних міжнародних організацій.

Міжнародний правопорядок можна визначити через три підходи (2008) (18):

1) як складну і динамічну систему взаємодій між різними державами, міжнародними організаціями, а також соціальними і національними спільнотами;

2) як результат регулювання інтересів держав і народів;

3) як умову і гарантію успішного міжнародного співробітництва в різних сферах людської діяльності.

Питання, пов'язані з глобальною та міжнародною безпекою, посідають чільне місце в наукових дослідженнях. Зміни у глобальному безпековому середовищі, поява нових та посилення традиційних загроз зумовлюють необхідність нових підходів до подолання недосконалості існуючих систем безпеки та їх неадекватності новим умовам.

Сучасні концепції терміну «безпека» різняться і відображені в керівних документах, що стосуються національної та міжнародної безпеки. Так, можна виділити чотири основні групи визначень (21):

1. Безпека як відсутність небезпеки (безпеку слід розглядати як стан відсутності небезпеки. Важливо зазначити, що наявність небезпеки не обов'язково означає відсутність безпеки, але безпека може сприйматися як відповідь на загрозу).

2. Безпека як невід'ємна властивість системи (цей підхід розглядає безпеку як невід'ємну властивість будь-якої системи. Нормальне функціонування будь-якої системи передбачає її певну захищеність від потенційно шкідливих впливів).

3. Безпека як результат певної діяльності (ця група визначень розглядає безпеку як мету, а не як діяльність. Це означає, що безпека досягається за допомогою конкретних заходів і дій, насамперед тих, що здійснюються державними інституціями).

4. Безпека як певний стан (цей підхід розглядає безпеку як певний стан, який, у свою чергу, можна розділити на три аспекти: стан відносин між суб'єктами; стан соціальної системи; стан нації, коли вона здатна протистояти різним загрозам і зберігати свій суверенітет).

В науковому середовищі більшого значення надається переважно визначенню міжнародної безпеки. Доцільно уточнити співвідношення понять «міжнародна безпека» та «глобальна безпека». Під міжнародною безпекою розуміють систему міжнародних відносин, засновану на дотриманні всіма державами загальновизнаних принципів і норм міжнародного права (і прийнятті міжнародних зобов'язань), що виключає вирішення спірних питань і розбіжностей силою або загрозою її застосування. У той же час, поняття «глобальна безпека» є ширшим за поняття «міжнародна безпека», адже глобальна безпека охоплює не лише аспекти міжнародних відносин та міждержавної безпеки, але й питання, пов'язані із загальним станом планети, загрозами здоров'ю та безпеці людини, екологічними проблемами, кібербезпекою, боротьбою з тероризмом, транснаціональною злочинністю та іншими глобальними викликами (21).

Міжнародна безпека, в свою чергу, зазвичай стосується питань безпеки між державами і в міжнародних відносинах. Глобальна безпека охоплює ширший спектр загроз і викликів, які можуть виникати з різних джерел, і включає аспекти, що впливають на безпеку всієї світової спільноти.

Залежно від масштабу проявів, традиційно виділяють: національний рівень, регіональний рівень та глобальний рівень міжнародної безпеки. Так, суттєві зміни у глобальному безпековому середовищі спонукають окремі держави та міжнародні організації розробляти та впроваджувати нові та вдосконалені ціннісні орієнтації, стратегії та рішення.

Варто зазначити, що більшість країн світу беруть участь у міжнародних організаціях. Як важливий елемент системи міжнародних відносин, глобальна організація пройшла довгий і складний шлях становлення та трансформації. Це призвело до неоднозначності в оцінках і визначеннях поняття «міжнародна організація» та його смислового наповнення. Перш за все, міжнародні організації являють собою специфічну форму співпраці та організації між різними країнами світу. Важливо підкреслити, що діяльність міжнародних організацій є вирішальним фактором у сучасному світі і відіграє ключову роль у зміцненні міжнародного співробітництва та впливі на глобальні проблеми.

Саруші Д. (18) визначає міжнародні організації як об'єднання держав, створені та діючі на основі міжурядових угод, з одного боку, і створені для виконання конкретних завдань (з відповідною метою), з іншого боку. Природно, що їхня діяльність регулюється

загальновизнаними принципами і нормами міжнародного права. Суттєвою особливістю міжнародних організацій є їхня здатність об'єднувати діяльність різних суб'єктів і виходити за межі національних кордонів для вирішення глобальних проблем і досягнення глобальних цілей.

Міжнародну організацію можна охарактеризувати як об’єднання держав, створену на основі міжнародного договору для досягнення конкретних цілей або завдань. Така організація, як правило, має постійні органи, відповідальні за реалізацію цих цілей і завдань.

Варто виділити характеристики, що притаманні міжнародним організаціям:

1. Членство трьох або більше країн: зазвичай складаються з більш ніж двох держав-членів, що відрізняє їх від двосторонніх угод або інших відносин.

2. Засновані на міжнародному праві: створюються на основі міжнародних угод і статутів, що дозволяє їм діяти відповідно до загальновизнаних принципів і норм міжнародного права.

3. Повага до суверенітету та невтручання: члени організацій зобов'язані поважати суверенітет і утримуватися від втручання у внутрішні справи інших членів-учасників.

4. Організаційна структура: мають організаційну структуру, яка включає керівні органи, комітети, секретаріати та інші підрозділи.

5. Конкретні цілі: мають визначені цілі або завдання, які визначають їхню діяльність та можуть охоплювати координацію дій держав у певній сфері, такій як політика, економіка, соціальний розвиток, військове співробітництво (11).

Вищезазначені характеристики допомагають ідентифікувати та відрізняти міжнародні організації від інших форм міжнародного співробітництва, таких як коаліції, союзи чи інші міжурядові об'єднання. Правовою основою діяльності міжнародних організацій є міжнародні договори, укладені державами-членами. Зокрема, такий міжнародний договір виконує роль статуту міжнародної організації та визначає ключові аспекти, такі як мета, принципи діяльності, структура, процедури та інші суттєві питання. Укладення міжнародного договору міжнародною організацією є найважливішим доказом її міжнародної правосуб'єктності.

Сьогодні міжнародні організації є ключовими об'єднаннями на міжнародній арені. Однією з перших міжнародних організацій вважається Ліга Націй, створена в 1919 році відповідно до положень Версальської системи договорів. Основний документ Ліги Націй був створений спеціальною комісією на Паризькій мирній конференції 1919-1920 років і підписаний 44 державами. Згідно зі Статутом, головною метою Ліги Націй був розвиток співробітництва між державами та гарантування їхнього миру і безпеки. В основному документі були викладені правила, що регулюють діяльність організації, та фундаментальні

принципи, яких повинні були дотримуватися всі держави-члени Ліги. Хартія зосередилася на питаннях роззброєння (статті 8, 9), намагаючись створити певну систему міжнародного контролю. Крім того, Статут регулював політичні та правові механізми мирного вирішення міжнародних спорів.

Ліга Націй приділяла значну увагу таким питанням, як захист меншин, захист прав вразливих груп населення, в тому числі жінок і дітей, захист прав біженців, захист жертв збройних конфліктів, права дітей. Ліга Націй припинила своє існування у 1946 році. Незважаючи на те, що вона не виконала своєї місії щодо запобігання війні та мирного врегулювання конфліктів, вона відіграла важливу історичну роль (10).

На сьогодні Організація Об'єднаних Націй (ООН) посідає провідне місце у світі. Це глобальна, універсальна, багатофункціональна міжурядова організація, заснована в 1945 році, яка наразі об'єднує 193 країни-члени. ООН є дійсно ключовою міжнародною організацією, що охоплює майже всі суверенні держави світу. ООН має складну організаційну структуру та постійні органи (включаючи Генеральну Асамблею, Раду Безпеки, Економічну та Соціальну Раду, Раду з опіки, Секретаріат, Міжнародний Суд та інші). Головним завданням ООН є підтримка міжнародного миру та безпеки.

Різноманітні завдання ООН включають різні спеціалізовані установи, кожна з яких працює у певній сфері. Традиційно, залежно від сфери діяльності, спеціалізовані установи ООН поділяються на три основні групи (16):

Перша група складається з економічних спеціалізованих установ. До цієї групи належать організації та фонди, що займаються розвитком і координацією економічних зусиль між державами. До них належать Міжнародний банк реконструкції та розвитку (МБРР), Міжнародний валютний фонд (МВФ), Міжнародна фінансова корпорація (МФК), Міжнародна асоціація розвитку (МАР) та інші організації, які співпрацюють у сфері фінансів, розвитку та економічної стабільності.

До другої групи належать соціальні спеціалізовані установи. До цієї групи належать організації, що працюють у сферах охорони здоров'я, праці, освіти та соціального розвитку. Це Міжнародна організація праці (МОП), Всесвітня організація охорони здоров'я (ВООЗ) та інші, які працюють над покращенням умов життя та добробуту населення.

Третю групу складають гуманітарні та культурні спеціалізовані установи. До цієї групи належать організації, що займаються гуманітарною допомогою, культурним обміном та іншими аспектами глобального співробітництва. Серед них - Дитячий фонд ООН (ЮНІСЕФ), ЮНЕСКО (організація ООН з питань освіти, науки і культури) та інші організації.

Варто зазначити, що зі змінами у глобальному безпековому середовищі Організація Об'єднаних Націй (ООН) приділяє більше уваги питанням безпеки. Насамперед, у квітні 2014 року Рада Безпеки ООН прийняла резолюцію щодо міжнародного миру і безпеки та реформування сектору безпеки. Реформа сектору безпеки в постконфліктних країнах має важливе значення для стабілізації та постконфліктного відновлення (14).

Діяльність Європейського Союзу (ЄС) є, насамперед, результатом кількох десятиліть зусиль, спрямованих на інтеграцію Європи. Необхідність відбудови Європи та забезпечення мирного співіснування народів після закінчення Другої світової війни породила ідею створення європейської спільноти. ЄС, до складу якого зараз входять 28 європейських країн, базується на спільних універсальних і демократичних цінностях і має на меті досягнення стабільності та миру.

Найважливішими інституціями ЄС, які відіграють ключову роль у його діяльності, є:

- Європейська комісія (виконує функції виконавчої влади ЄС і відповідає за реалізацію законів і політики ЄС).

- Рада Європейського Союзу (Рада міністрів) (складається з представників кожної країни-члена, зазвичай міністрів). Рада розглядає і приймає рішення з різних питань, включаючи законодавство ЄС, бюджет і зовнішню політику).

- Європейська Рада (найвищий політичний орган ЄС, що складається з глав держав та урядів країн-членів. Вони визначають загальну стратегію ЄС і вирішують ключові питання).

- Суд Європейського Союзу (відповідає за вирішення правових спорів, що виникають із законодавства ЄС, і забезпечує послідовне тлумачення законодавства).

- Європейський центральний банк (відповідає за монетарну політику і валюту Єврозони, а також за підтримку стабільності фінансової системи).

- Європейський парламент (обирається європейськими громадянами; є представницьким органом ЄС і має повноваження приймати рішення щодо законодавства, бюджету та інших питань) (13).

Ці інституції працюють разом, щоб формулювати та впроваджувати політику і забезпечувати ефективне функціонування ЄС як наднаціональної організації.

Неможливо оминути увагою головну організаційну структуру механізму цивільного захисту ЄС - Координаційний центр з реагування на надзвичайні ситуації (ERCC). Він забезпечує швидке та скоординоване реагування на надзвичайні ситуації як всередині, так і за межами Європейського Союзу. ERCC допомагає країнам-членам ЄС та іншим країнам у боротьбі з надзвичайними ситуаціями та катастрофами, координуючи зусилля з реагування та надаючи необхідну допомогу.

Рада Європи - це міжурядова організація, діяльність якої спрямована на захист прав людини та верховенства права. Рада функціонує починаючи з 1949 року і є першою європейською міжурядовою організацією, створеною після Другої світової війни. Серед 46 держав-членів РЄ є і Україна. Визнання верховенства права та захист прав людини і основоположних свобод є ключовими умовами для вступу країни до РЄ.

Цілі РЄ включають в себе наступні:

1. Сприяння тіснішим зв'язкам між європейськими країнами.

2. Перетворення Європи на демократичний простір.

3. Захист прав людини.

4. Координація діяльності та розвитку в рамках Ради у співпраці з іншими європейськими державами (4).

Рада Європи розглядає широке коло питань, що стосуються спільних інтересів її країн-членів, і впроваджує різні ініціативи та заходи для досягнення своїх цілей. Це охоплює роботу в галузі економіки, соціальної справедливості, культури, науки, права та захисту прав людини, серед багатьох інших.

Європейська конвенція з прав людини (ЄКПЛ) (2021) - одна з найважливіших міжнародних конвенцій у сфері прав людини та основоположних свобод. Вона була прийнята Радою Європи з метою захисту прав і свобод громадян на території європейських країн-членів та охоплює широке коло прав і свобод: право на життя, свободу думки, совісті, релігії, праці, права в судовому процесі, серед багатьох інших (7).

Організація з безпеки і співробітництва в Європі (ОБСЄ) є найбільшою у світі регіональною міжурядовою організацією, що займається питаннями безпеки, які охоплюють військово-політичний, економічний, екологічний та гуманітарний виміри. Сьогодні ОБСЄ об'єднує 57 країн-учасниць з Європи, Азії та Північної Америки. Зусилля Альянсу спрямовані насамперед на підтримку миру і безпеки, протидію новим викликам і загрозам, забезпечення стабільності та процвітання країн-членів організації.

Основні напрямки діяльності ОБСЄ включають:

- миротворчі операції (бере участь у різних миротворчих місіях з метою врегулювання конфліктів і відновлення стабільності в різних регіонах світу)

- протидія загрозам (бореться з різними міжнародними загрозами, такими як тероризм, розповсюдження зброї масового знищення, торгівля людьми та інші).

- освітні та наукові програми (підтримує освітні та наукові ініціативи з метою сприяння розвитку знань та досліджень у сфері безпеки та оборони).

- гуманітарна допомога (може надавати гуманітарну допомогу країнам, що постраждали від стихійних лих та техногенних катастроф).

- підтримка демократії (сприяє розвитку демократичних інститутів у різних країнах).

- захист прав людини (визнає захист прав людини важливою частиною своєї діяльності).

- боротьба з корупцією (працює над тим, щоб сприяти чесності та прозорості в державних установах).

- ефективне управління (розробляє механізми ефективного управління та прийняття рішень) (1).

Організація Північноатлантичного договору (НАТО) - міжнародна військово-політична організація, створена у 1949 році. Сьогодні НАТО є однією з провідних складових глобальної безпеки. Її головна місія полягає в захисті свободи і безпеки всіх її членів політичними і військовими засобами відповідно до принципів Статуту Організації Об'єднаних Націй. НАТО складається з 33 країни-члена. Відповідно до Північноатлантичного договору (1949), Альянс відкритий для інших європейських країн, які бажають дотримуватися його принципів і безпосередньо сприяти безпеці Північноатлантичного регіону (20).

Договір, який є основою для створення Альянсу, є важливим правовим документом, що регулює функціонування та співробітництво країн-членів НАТО. Кожна країна-член НАТО добровільно приєднується до цього договору після внутрішнього громадського обговорення та схвалення у своїй країні відповідно до її законів і процедур.

Основною метою цього договору є забезпечення безпеки та взаємодопомоги між державами-членами у випадку агресії або загрози агресії. Це означає, що кожна держава зобов'язується надавати допомогу іншим членам Альянсу в разі агресії або її загрози. Договір також містить положення, що забороняють країнам-членам брати на себе міжнародні зобов'язання, які не відповідають договору. Він забезпечує єдність і координацію дій держав-членів у сфері безпеки і оборони.

Скандинавські країни мають дуже чітку стратегію стосовно формату співробітництва з різними міжнародними організаціями: членства, асоціації, інтеграції. Це стосується як ЄС, НАТО, так і участі в роботі інших регіональних організацій. Так, Швеція і Фінляндія є активними партнерами НАТО, не будучи його членами. Але таке співробітництво не може бути ефективним лише на короткостроковій основі. Для цього необхідна певна національна стратегія досягнення цілей, яких ви бажаєте досягти.

2. Вплив міжнародних організацій на формування, забезпечення та зміцнення світового правопорядку та безпеки

Роль міжнародних організацій у підтриманні миру і безпеки сьогодні є багатогранною і різноманітною, розвивається міжнародне співробітництво і координація зусиль міжнародних організацій щодо зміцнення миру і безпеки. Водночас їхня діяльність багато в чому залишається недостатньо ефективною, що на сьогодні є об'єктивною обставиною, яка відображає поворот держав до ідей їхнього суверенітету.

На думку політичних експертів у галузі геополітики та міжнародних досліджень, центральною проблемою міжнародних відносин є проблема порядку - його конституювання, руйнування та відновлення.

Завершення біполярного протистояння відкрило нові можливості для конструктивної співпраці між державами на регіональному та глобальному рівнях, в рамках ООН та інших міжнародних організацій. Загроза глобального конфлікту попереднього типу теоретично має бути зведена до мінімуму, але стає очевидним, що майже всі інституційні механізми підтримання міжнародної безпеки, створені після Другої світової війни та за часів холодної війни (ООН, НАТО, ОБСЄ), не є адекватними, а подекуди й безпорадними перед викликами та загрозами нового століття. Спроби реформувати ці структури поки що не увінчалися успіхом. Також відсутня політична воля до створення нових, більш ефективних структур міжнародної безпеки. Як наслідок, рівень керованості міжнародних криз і процесів різко падає. Можна припустити, що опосередковано, а саме зниження ефективності діяльності міжнародних організацій у забезпеченні глобального правопорядку стало однією з ключових причин суттєвого зростання конфліктогенності сучасного геополітичного ландшафту, а також появи в ньому ентропійних процесів (6).

Згідно з Індексом конфліктності ACLED (2023), за останні 12 місяців кількість інцидентів політичного насильства зросла на 27%, і, за оцінками, кожна шоста людина наразі зазнала впливу конфлікту.

Вперше Індекс конфліктності було опубліковано в січні 2023 року, а в липні 2023 року його було оновлено за зміненою методологією. Світова карта рейтингу індексу конфліктності представлена на рис. 1.

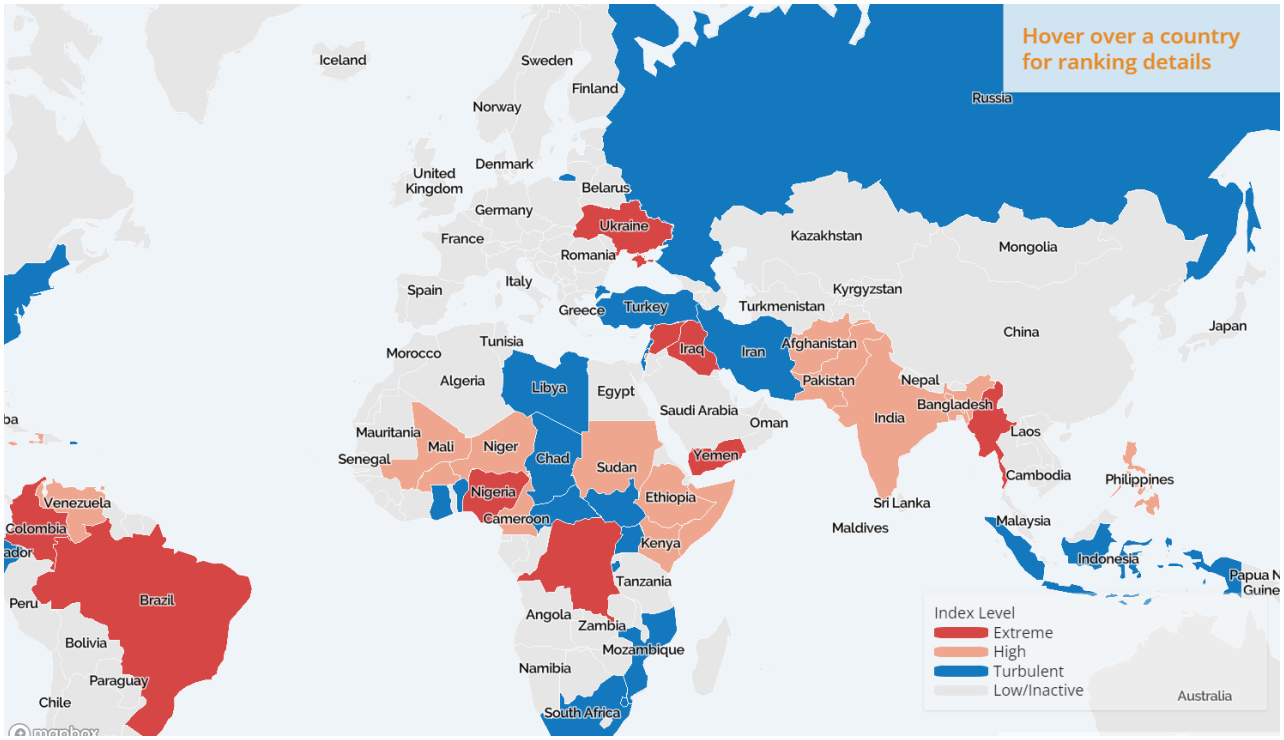


Рис. 1. Світова карта рейтингу індексу конфліктності

Джерело: Індекс конфліктів ACLED, 2023 (8)

Конфлікт є складним і широко розповсюдженим явищем. У 2022 році у світі відбулося понад 125 700 подій, пов'язаних з політичним насильством, в результаті яких загинуло понад 145 500 осіб. У 2023 році відбулося на 12% більше конфліктів порівняно з 2022 роком, а ACLED фіксує зростання на понад 40% порівняно з 2020 роком. Кожна шоста людина живе в зоні активного конфлікту. У 234 країнах і територіях, охоплених ACLED, у більшості з них - 168 - у 2023 році стався щонайменше один випадок конфлікту. Зафіксовано понад 147 000 конфліктних подій і щонайменше 167 800 смертей (8).

Ці інциденти варіювалися від нападів натовпу на прихильників політичних партій і вбивств представників місцевої влади до державних убивств, повстанських сутичок і насильства з боку картелів. В одній і тій самій країні часто відбуваються одночасно кілька видів насильства, що наражає суспільство і державу на кілька одночасних загроз. З метою мінімізації цих загроз, всі зацікавлені сторони, включаючи політиків, аналітиків, організації громадянського суспільства, бізнес та ЗМІ, потребують неупередженої, прямолінійної та надійної оцінки серйозності конфлікту. Визначення того, які країни відповідають певному пороговому рівню серйозності конфлікту, має відчутні наслідки для того, які види насильства будуть помічені і на які з них реагувати - і де саме. Такий показник має враховувати

різноманітні місцеві складнощі та виокремлювати важливі закономірності, які можуть бути використані при прийнятті стратегічних та оперативних рішень.

Конфлікти відрізняються за своєю інтенсивністю, частотою та формою. Тому порівняння кількості подій може призвести до викривлення результатів. Спираючись на найновіші дані та закономірності, в оновленому Індексі конфліктів ACLED за 2024 рік оцінюється рівень конфліктів за чотирма ключовими показниками: смертоносність, небезпека для цивільного населення, географічне поширення конфлікту та фрагментація збройних угруповань.

Країни ранжуються за кожним з цих чотирьох показників, і ці позиції визначають загальне місце в Індексі. Місце країни в Індексі відображає рівень її конфліктності порівняно з іншими країнами.

Рівень конфліктності існує в широкому діапазоні, і певний рівень конфліктів спостерігається майже в кожній країні. Найвищий рівень конфліктності спостерігається у 50 країнах, що увійшли до списку Індексу (рис. 2). Ці країни класифікуються як «екстремальні», «високі» або «неспокійні». На ці 50 країн, що увійшли до рейтингу, припадає 97% усіх конфліктних подій, зафіксованих за останні 12 місяців. На країни з надзвичайно високим рівнем насильства припадає 40% усіх конфліктів.

Із 50 країн в рейтингу рівнів насильницьких конфліктів у світі М'янма є найбільш насильницькою в цілому і зберігає свою позицію найбільш «фрагментованої» через сотні дрібних ополченців, сформованих для боротьби з урядом після перевороту в 2021 році. Сирія є другою найбільш конфліктною країною через численні конфлікти, що накладаються один на одного, які продовжують відбуватися в межах її кордонів. Палестина має конфлікт, що охоплює майже всі її території, і тому вважається найбільш «дифузним» конфліктом.

Позиція Палестини покращилася з моменту складання останнього Індексу, що повністю пояснюється тривалою і смертоносною війною з Ізраїлем, яка ведеться переважно в секторі Газа. Мексика залишається найнебезпечнішою країною для своїх громадян, оскільки вони є безпосередньою мішенню картелів у їхній жорстокій конкурентній боротьбі. Україна залишається найсмертоноснішою країною, оскільки армії як з українського, так і з російського боку втратили десятки тисяч бійців за понад два роки воєнної агресії росії проти України.

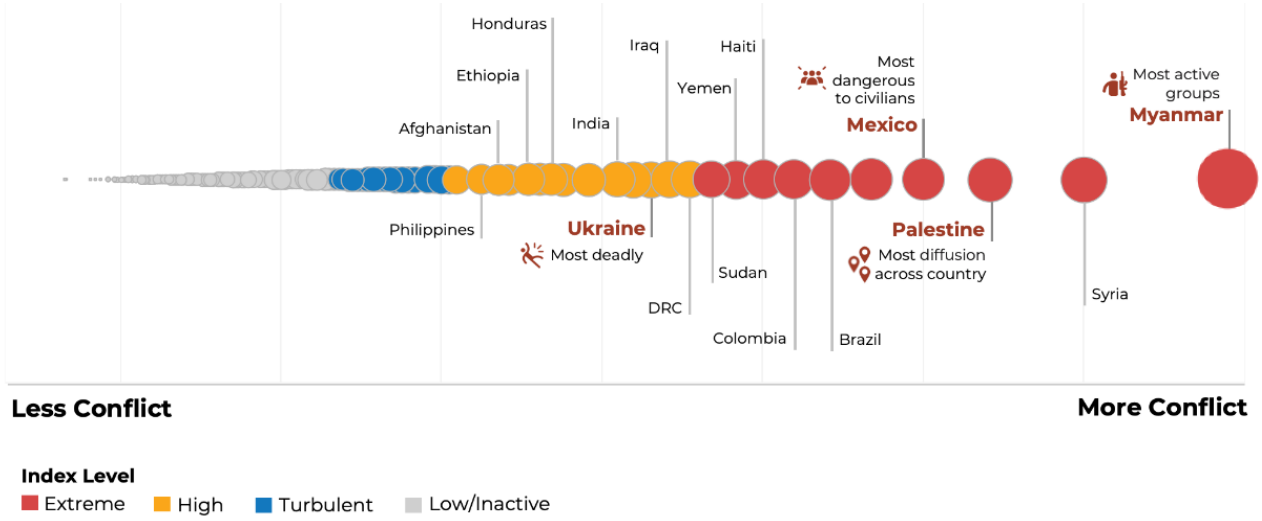


Рис. 2. Індекс конфліктів: рейтинг рівнів насильницьких конфліктів у світі

Джерело: Індекс конфліктів ACLED, 2023 (8)

Багато існуючих індексів ґрунтуються на підрахунку подій і кількості загиблих, які часто можуть спотворювати масштаби і наслідки конфлікту для різних громад і держав. Інші зосереджуються на характеристиках і оцінках «нестабільності» і недостатньо враховують політичне насильство та його різновиди. У 2022 році найбільш інтенсивні рівні насильства, виміряні лише за загальною кількістю подій, були зафіксовані в Україні (понад 34 400 подій), Сирії (понад 10 400), М'янмі (понад 9 300), Бразилії (понад 7900), Мексиці (понад 7 100) та Ємені (понад 6400). Країни з найбільшою кількістю смертей, пов'язаних з конфліктом, - це Україна (понад 28 000 смертей), М'янма (понад 19 000), Нігерія (понад 10 600), Мексика (понад 7 700) та Ємен (понад 6 700). Україна посідає перше місце в обох списках через руйнівний конфлікт між російськими та українськими збройними силами. Багато інших країн пережили велику кількість подій і загиблих через більш різноманітні насильницькі обставини.

Останніми роками світ стає все більш жорстоким: кількість конфліктних подій зросла більш ніж на 40% з 2020 по 2023 рік; у 2023 році вона збільшилася на 12% порівняно з 2022 роком. Але 2020 рік був відносно менш насильницьким порівняно з 2018-2019 роками, коли вирували війни в Афганістані та Сирії. Порівняно з цими роками, зростання у 2023 році все ще є значним - в середньому на 20%. Станом на січень 2024 року 15 країн покращили свої позиції в Індексі за п'ятирічний період з 2019 по 2023 рік, а в 16 країнах рівень конфлікту погіршився. Шістнадцять країн постійно залишаються в категоріях «екстремально високого» або «високого» рівня конфлікту без змін у період з 2019 по 2023 рік. Загалом, з 50 країн, що посідають перші місця в Індексі, більше половини (42) переживають сталий або зростаючий рівень конфлікту порівняно з 2019 роком.

Позиція України в Індексі конфліктності знизилася з двох причин. По-перше, в українському конфлікті спостерігається значний рівень стагнації, в тому числі щодо кількості загиблих, активних бойових дій та воюючих сторін. Наразі конфлікт в Україні перебуває на стадії виснаження, без жодних ознак завершення і з дуже незначними ознаками змін. По-друге, конфлікти в інших країнах зростають за багатьма показниками: частота подій, кількість конфліктуючих сторін та територій, на яких відбувається активний конфлікт. У той час як рівень конфліктності в Україні залишається відносно стабільним і послідовним, постійне зростання конфліктів в інших країнах означає, що він падає з «екстремального» до «високого».

Конфлікти зростають найшвидше в країнах із середнім рівнем доходу, що демократизуються. Країни з середнім рівнем доходу переживають найбільше зростання конфліктів. Бідність не є передвісником конфлікту, а багатство не є гарантією миру. На графіку нижче 50 країн, що посідають перше місце в Індексі конфліктності ACLED, розміщені відповідно до Індексу людського розвитку ООН. Як показує це порівняння, багато країн з «екстремальним» або «високим» рівнем конфліктів є країнами з високим і стійким рівнем економічного і соціального розвитку (рис. 3).

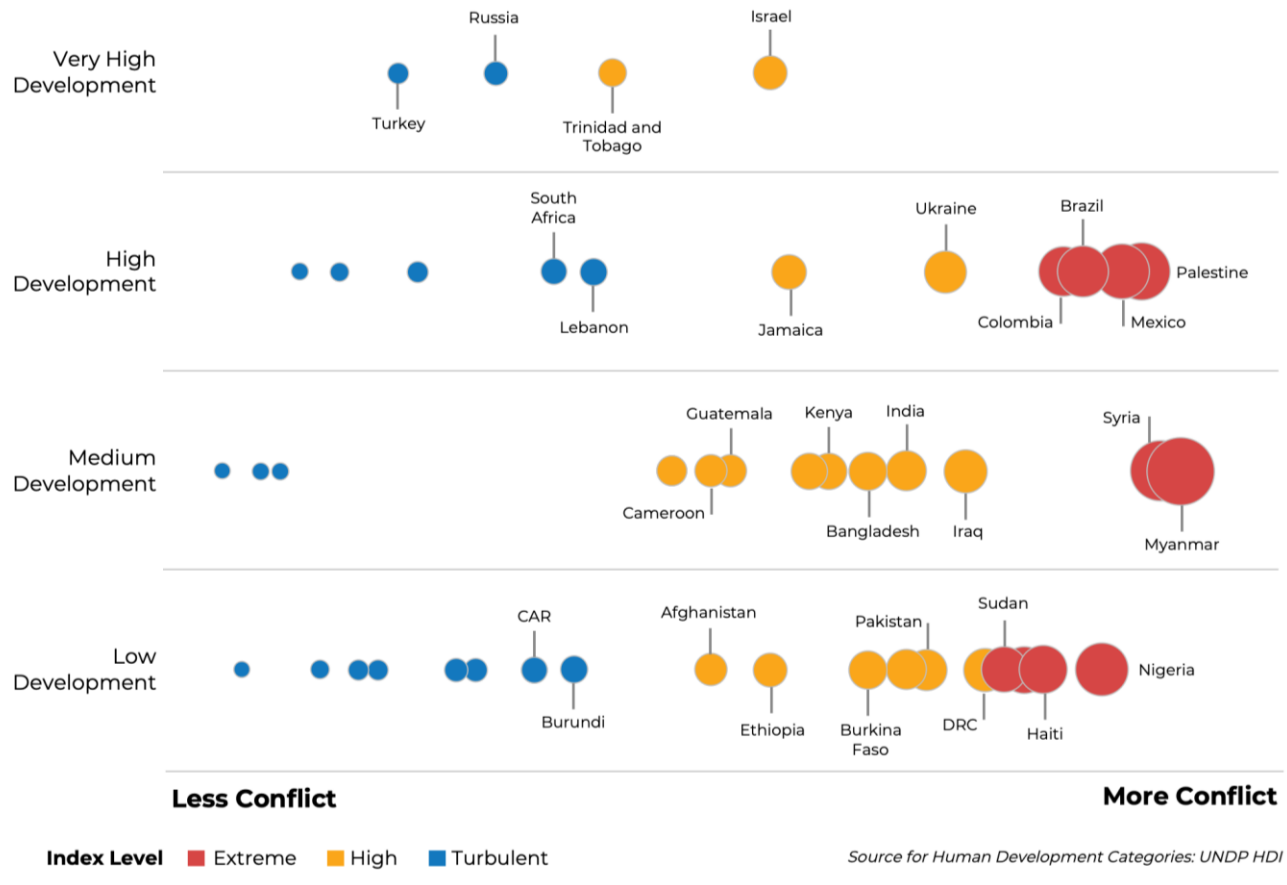


Рис. 3. Топ-50 країн за категоріями людського розвитку ООН

Джерело: Індекс конфліктів ACLED, 2023 (8)

Варто зазначити, що демократія не захищає країни від насильницької політики. У країнах, що переходять до демократії або регресують від демократії, нові форми і учасники політичної конкуренції сприяють виникненню конфліктів. Демократичні зрушення в усьому світі зменшили ймовірність традиційних громадянських війн і збільшили ймовірність діяльності ополченців і політичного насильства. Країни з «частково вільними» системами, за класифікацією *Freedom House*, проводять вибори, змінюють і усувають лідерів, мають інклюзивне представництво та інші ознаки демократії, але часто стикаються з високим рівнем політичного насильства. У 2024 році відбудеться безпрецедентна кількість виборів, і більше половини населення світу візьме участь у виборах або проживатиме в країні, де відбудуться вибори. Це призведе до насильницьких нападів на цивільних осіб і більш цілеспрямованих нападів і вбивств місцевих чиновників з боку озброєних груп.

Як відомо, більшість міжнародних конфліктів, що загрожують глобальній безпеці і миру, мають своїм джерелом або внутрішньодержавну, або регіональну нестабільність, викликану різними економічними (прагнення до перерозподілу енергоресурсів, продовольства, питної води), політичними (боротьба за владу і сфери впливу), етнічними (почуття національної переваги, заздрість, ворожнеча і неприязнь), релігійними (недостатня духовна і моральна зрілість конфліктуючих народів), а також іншими чинниками (пов'язаними, наприклад, з тероризмом, екстремізмом). Тому передбачуваний конституційно запрограмований і гарантований механізм раннього попередження і мирного (правового) розв'язання міжнародних конфліктів і проблем має ґрунтуватися, насамперед, на розумінні та аналізі причин і природи різного роду протистоянь і джерел небезпеки (15).

У сучасних умовах система міжнародної безпеки включає сукупність основоположних принципів безпеки, міждержавних механізмів і структур, міжнародно-правових норм, багатосторонніх договорів та інших елементів, створених і функціонуючих з метою запобігання військовим зіткненням, їх локалізації, врегулювання політичних, економічних і військово-стратегічних протиріч політичним шляхом, а також особливий режим контролю за міжнародною, особливо військовою, діяльністю і відповідний інформаційний режим. Найбільш значну роль у забезпеченні міжнародної безпеки відіграють міждержавні інститути з внутрішньою жорсткою структурою, органами координації та контролю, чітко вираженою політикою у військово-політичному та економічному плані, в яких «питома політична, економічна та військова вага» їх учасників є значною (21).

Іноді своєчасне виявлення, розпізнавання та діагностика національних і регіональних проблем, які можуть стати початком тих чи інших глобальних конфліктів, може бути не менш

складним завданням, ніж їх законне і мирне вирішення. Будь-яка глобальна проблема для свого вирішення, як правило, вимагає обов'язкової участі та легітимної і скоординованої волі всіх зацікавлених і залучених до даного конфлікту держав. Міра ефективності запобігання і своєчасного вирішення глобальних проблем, пов'язаних зі збереженням міжнародного миру і безпеки, багато в чому залежить від успішності підтримки постійного діалогу між територіально або політично пов'язаними державами, від вироблення спільних позицій і довгострокових інтересів в їх різноманітному релігійному, політичному та економічному житті, а також способів їх повсякденного співіснування.

Варто виокремити, основні фактори, що вплинули на зростання світових оборонних витрат: військові операції в Іраку, Єгипті, Лівії, Сирії та інших країнах Близького Сходу; збільшення військової присутності США в різних частинах світу; повернення росії на глобальну світову арену, а також зростання могутності Китаю, який претендує на лідерство. Ці фактори стали каталізаторами в контексті загального підвищення рівня напруженості в сучасному світі (21).

Не менш вагомий внесок у цю кризу вносить відсутність консолідованої політики постійних членів Ради Безпеки ООН щодо фактичних та потенційних країн-порушників режиму нерозповсюдження ядерної зброї, включаючи прийняття ефективних політичних, дипломатичних та економічних санкцій. Це, наприклад, стосується КНДР, керівництво якої "вміло" грає на протиріччях між провідними країнами світу і, по суті, ігнорує резолюції РБ ООН. Відповідно, зростає загальна нервозність і військово-політична нестабільність. У деяких держав з'явиться спокуса завдати превентивних ударів, яскравим прикладом чого є широкомасштабне вторгнення росії в Україну 24 лютого 2022 року.

Наразі існує потреба у розробці комплексної довгострокової стратегії у сфері нерозповсюдження конфліктного потенціалу, стратегії, що синтезує дипломатичні, економічні та інші заходи. Пріоритетом має стати розвиток нових глобальних і регіональних структур безпеки, вдосконалення взаємодії спецслужб і систем міжнародних гарантій безпеки, а також розвиток військових силових операцій, але як крайній засіб.

Незважаючи на останні тенденції, що свідчать про відновлення націоналізму і збереження актуальності національних кордонів, більш масштабні структурні зміни у світовій політиці в епоху цивілізаційного конфлікту продовжують вказувати на необхідність вирішення питань безпеки з урахуванням ситуації за межами просторових кордонів держави, тобто складних реалій світу, що глобалізується. Посилення зв'язків завдяки інформаційно-комунікаційним технологіям, а також інші позитивні аспекти глобалізації вимагатимуть від державних органів та інших суб'єктів постійних зусиль, спрямованих на вирішення проблем безпеки в «ненаціональних»

регіонах, що виходять за межі територіальних кордонів. Розмивання меж між зонами конфлікту і зонами миру зробить стримування і стратегічні дискусії менш ефективними, оскільки вони спираються на сприйняття держав як унітарних суб'єктів. Важливим питанням найближчим часом стане пошук шляхів співпраці задля покращення глобальної безпеки і стабільності в цьому новому середовищі без загрози для інших життєво важливих колективних благ, таких як громадянські свободи, недоторканність приватного життя і свобода пересування.

Міжнародне право, як і будь-яка інша правова система, не може обійтися без примусових заходів. Завдання полягає в тому, щоб удосконалити їх застосування. Наразі одним, але не однаково зрозумілим терміном «санкції» досить часто визначають по суті різні, хоча і взаємопов'язані правові явища, не тільки не розрізняючи їх, але навіть іноді намагаючись приписати їм властивості, якими вони не володіють. Дотримуючись надто широкого розуміння міжнародно-правових санкцій, багато юристів-міжнародників ототожнюють або плутають їх з формами міжнародно-правової відповідальності. Це розмиває межі між санкціями та відповідальністю, перешкоджає чіткому розумінню природи цих інститутів та правильному розумінню ролі кожного з них у системі міжнародно-правового регулювання.

Використання терміну «санкція» щодо поняття «примусовий захід невійськового характеру Ради Безпеки ООН» не може викликати абсолютного несприйняття, оскільки в такому випадку він нестиме смислове навантаження примусового засобу забезпечення зобов'язань держав за Статутом ООН, які, на думку спеціально уповноваженого органу цієї міжнародної організації, створюють загрозу міжнародному миру або безпеці. Ототожнювати ці санкції із заходами міжнародної відповідальності непродуктивно, оскільки Рада Безпеки ООН не є учасником правовідносин відповідальності, які складаються між державою-правопорушником і жертвою міжнародного правопорушення. Застосування невійськових санкцій Радою Безпеки ООН не упереджує можливості притягнення держави-правопорушника до міжнародної відповідальності в майбутньому (12) .

Експерти вважають, що вдосконалення діяльності Ради Безпеки має відбуватися, насамперед, шляхом перегляду методів і процедур її роботи. Запорукою ефективності цього органу є, серед іншого, постійна взаємодія із зацікавленими країнами (країнами-стейкхолдерами) та бездоганне правове забезпечення, включаючи суворе дотримання всіма учасниками міжнародного спілкування положень Статуту ООН щодо місця і значення Ради у підтриманні міжнародного миру і безпеки (12). Також видається необхідним подальший прогрес у роботі Комісії міжнародного права ООН з кодифікації питань міжнародної відповідальності та застосування примусових заходів.

З моменту створення Організації Об'єднаних Націй минуло понад 70 років, і на міжнародній арені відбулися значні зміни. ООН залишилася в основному незмінною, хоча деякі зміни все ж таки відбулися. У статті 1 Статуту ООН викладено чотири основні цілі організації. Ці цілі сформульовані універсально, вони позбавлені будь-якої конкретики. Але в нашу сучасну епоху ООН вирішує проблеми, які вимагають чіткості у формулюванні для досягнення більшої ефективності ООН. Рада Безпеки повинна активніше використовувати ресурси Військово-штабного комітету в підтримці міжнародного миру і безпеки шляхом створення регіональних допоміжних органів. Зокрема, доцільно створити комітет, який співпрацюватиме з регіональними міжнародними організаціями для забезпечення моніторингу потенційних конфліктних ситуацій у різних регіонах та їх попередження. Видається доцільним використання стейкхолдерського підходу, тобто збалансування інтересів для досягнення бажаних цілей у сфері світового правопорядку, виходячи з утилітарної парадигми, а не категоричних імперативів ідеології.

3. Особливості діяльність Ради Безпеки ООН у підтримці світового правопорядку та безпеки в сучасному світі та в Україні у період російсько-української війни

В умовах глобалізації та паралельних процесів дезінтеграції і регіоналізації успішність розвитку будь-якої держави, в т.ч. України, залежатиме від наявності ефективної стратегії взаємодії з міжнародними об’єднаннями, в рамках яких вона зможе робити посильний внесок у забезпечення миру, стабільності та розвитку на глобальному та регіональному рівнях, а також – використовувати інструменти міжнародного співробітництва та отримувати різноманітну допомогу для реалізації власних цілей.

Окремі європейські країни без формального членства в ЄС (Норвегія, Швейцарія) чи в НАТО (Австрія, Фінляндія, Швеція) є, по суті, інтегрованою частиною економіки ЄС і євроатлантичної безпекової спільноти.

Україна співпрацює з міжнародними організаціями в різних форматах і якостях (повноправний член, кандидат на членство, партнер, спостерігач, контрибутор) - сума членських внесків щорічно сягає близько $45 млн. Членство в 75 міжнародних організаціях може слугувати підтвердженням добрих намірів політичного керівництва держави співпрацювати «з усіма заінтересованими партнерами, уникаючи залежності від окремих держав, груп держав чи міжнародних структур».

Україна є активним контрибутором спільних заходів із зміцнення міжнародної стабільності та безпеки: бере участь у багатьох багатонаціональних місіях (п’яти – ООН, двох – ЄС, трьох – НАТО, одній (у Придністров’ї) – на засадах міжнародної угоди). У 2012р. збільшено загальний внесок України в міжнародні зусилля із врегулювання конфліктів шляхом розширення контингенту в чотирьох місіях ООН та одній – НАТО. 2013р. відзначився головуванням України

в ОБСЄ та ОЧЕС. Продовжується інтенсивне співробітництво з НАТО – на основі річних національних програм співробітництва з Альянсом. Готується до підписання Угода про асоціацію з ЄС.

Водночас Україна покладає великі надії на зміцнення власних спроможностей забезпечення національної безпеки (в т.ч. економічної, енергетичної, екологічної тощо), протидії сучасним викликам і загрозам за рахунок механізмів міжнародного співробітництва та залучення допомоги міжнародних організацій і країн-партнерів. Зовнішня консультативна, технічна, фінансова допомога (безповоротна фінансова допомога та кредити на вигідних умовах) також є критично важливими для проведення широкого спектру структурних, соціально-економічних і політичних реформ, реалізації стратегічно важливих проектів.

Україна як повноправний суб'єкт міжнародних відносин активно співпрацює з різними державами та міжнародними організаціями. Рівні відносин з кожною із сторін відрізняються за формою і змістом, оскільки з об'єктивних причин неможливо співпрацювати одночасно з усіма з однаковою інтенсивністю або гармонізувати відносини з партнерами, між якими існують глибокі двосторонні протиріччя.

Вибір міжнародних партнерів для співробітництва у сфері безпеки та подальший розвиток відносин великою мірою визначається спільністю (близькістю, збігом) цілей, інтересів, оцінок загроз і підходів до протидії їм. Оцінки експертами відповідних критеріїв демонструють систему координат, в якій вони бачать Україну. Очевидно, що найбільш прийнятним і вигідним для держави має бути співробітництво з організаціями, де спостерігається найвища спільність позицій (ООН, ОБСЄ, ЄС). Не можна, звичайно, вилучати із списку тих партнерів, у співробітництві з якими відзначається лише часткова спільність позицій (ОДКБ, Митний союз), але слід бути готовим до суттєвих обмежень.

Узагальнюючи окремі оцінки експертів (спільності/ збігу позицій України та міжнародних організацій, з якими вона співпрацює, важливості для неї цілей та окремих сфер безпекового співробітництва, ефективності його форм), міжнародні організації можна умовно поділити на дві групи. Перша – ООН, ОБСЄ, ЄС, НАТО. Друга – СНД, ОДКБ, Митний союз. Такий поділ зумовлений наступними аспектами. По-перше, на думку експертів, найбільшою мірою цінності, інтереси, позиції та підходи України збігаються з цінностями, інтересами, позиціями та підходами організацій першої групи, тоді як з позиціями організацій другої групи збіг є значно меншим. По-друге, співробітництво з організаціями першої є відносно більш важливим і продуктивним для України, зокрема – для зміцнення її безпеки та обороноздатності, підвищення міжнародного авторитету, зміцнення демократії, поглиблення відносин з ЄС, розвитку економіки, подолання корупції і підвищення добробуту громадян.

Експертні оцінки співробітництва з міжнародними організаціями другої групи є помітно нижчими (12).

Проаналізувавши експертні оцінки важливості безпекового співробітництва за його цілями, можна визначити, що до першої трійки рейтингу увійдуть ЄС, НАТО, ОБСЄ. Оцінюючи вплив безпекового співробітництва на реалізацію його цілей, експерти віддають перевагу співробітництву з ЄС, НАТО, ОБСЄ та ООН. Експертні оцінки ефективності різних форм безпекового співробітництва підтверджують загальний висновок стосовно умовного рейтингу міжнародних безпекових організацій. Найбільш результативним за всіма параметрами є партнерство з НАТО. Відповідно, експерти віддають помітну перевагу спільним військовим навчанням, співробітництву в рамках операцій та місій, підготовці військових і цивільних фахівців у сфері безпеки саме з Альянсом – провідною політико-військовою організацією у світі. Половина опитаних експертів переконані, що саме НАТО має бути провідною організацією в забезпеченні безпеки в Європі, що значно переважає частку тих, хто бачить у цій ролі ОБСЄ (22,5%) та ЄС (17,5%). Цю картину доповнюють оцінки важливості співробітництва України з міжнародними організаціями в різних секторах безпеки – оборонній реформі, протидії тероризму, нерозповсюдженні зброї масового ураження (ЗМУ), протидії новим загрозам, подоланні наслідків надзвичайних ситуацій. За всіма параметрами експерти віддають пріоритет НАТО, ЄС, ООН, ОБСЄ. Дещо нижче оцінюється важливість партнерства з СНД, ОДКБ і ШОС.

Міжнародна безпека є запорукою глобального самозбереження та розвитку. Суб’єктами міжнародної безпеки є міжнародні організації, метою яких є забезпечення дотримання безпеки. Міжнародні організації займаються широким спектром питань безпеки, включаючи контроль над озброєннями, попередження конфліктів, забезпечення прав і свобод людини і громадянина.

Сьогодні для України важлива співпраця, підтримка та посередництво міжнародних організацій у врегулюванні воєнного конфлікту. Першість у порядку розв’язання збройних конфліктів в Україні належить Організації Об’єднаних Націй (ООН) – головній міжурядовій міжнародній організації, яка підтримує мир і безпеку у всьому світі.

Україна є однією з держав-засновниць Організації Об'єднаних Націй і є повноправним членом організації, беручи активну участь у всіх її заходах та ініціативах. Включення України до складу непостійних членів Ради Безпеки ООН на початку 2000-2001 років можна назвати історично значущою подією, яка визначила її активну роль на міжнародній арені. Цей крок засвідчив визнання впливу України та її готовність долучитися до міжнародних зусиль, спрямованих на збереження міжнародного миру та безпеки. Членство в Раді Безпеки ООН дозволяє державі брати активну участь у прийнятті доленосних рішень та посилює її роль у

формуванні глобальної політики. Участь України в Раді Безпеки ООН підкреслила її відданість принципам демократії, верховенства права та глобальної стабільності, зробивши вагомий внесок у світове міжнародне співтовариство (17).

Повномасштабне вторгнення росії в Україні 24 лютого 2022 року, похитнуло безпекову ситуацію в Європі та в усьому світі. Цю війну вже названо найбільшим з часів Другої світової війни збройним конфліктом у Європі. Терористична та військова загроза зі сторони рф та союзних їй держав поширилася по всьому світу та спалахнула напруженням навколо Тайваню, погрозами ядерних ударів зі сторони КНДР та росії, агресивними діями Ірану в регіоні.

Настільки складна й напружена обстановка у світі, який опинився на порозі Третьої світової війни та ядерної катастрофи, вимагає максимальної мобілізації всіх наявних дипломатичних, політичних та правових ресурсів, які дозволили б знизити напругу та віднайти ефективні механізми припинення агресивної терористичної політики вказаних країн. Одним із головних органів ООН, який покликаний вирішувати проблеми міжнародної безпеки, є Рада Безпеки ООН.

2022 рік став кризовим для світу та ООН – адже військова агресія росії проти України спричинила великі руйнування на території України, загибель безлічі не тільки військових, але й цивільних осіб. Російська злочинна армія вчинила та вчиняє безліч злочинів геноциду українського народу на окупованих територіях, примусово вивозить цивільних осіб на свою територію, вбиває та катує військовополонених. Росія неодноразово створювала загрозу ядерної, хімічної катастрофи на території України, а її ракетні обстріли не лише нищать житлові будинки та інфраструктуру України, але й загрожує сусіднім країнам – Молдові та Польщі, на території яких уже прилітали російські ракети. Водночас вся Європа стикнулася з новою міграційною кризою, спричиненою великими потоками біженців з України. Очевидно, що станом на кінець 2022 року міжнародні організації, включно з Радою Безпеки ООН мають проблеми з застосуванням тих механізмів забезпечення миру в світі, які вони мають у своєму арсеналі. Відтак, виникає необхідність аналізу ефективності цього колективного органу в урегулювання військової агресії РФ в Україні.

Згідно з положеннями Статуту ООН, підтримання миру і безпеки у світі повинно будуватися на базі загальновизнаних принципів і норм міжнародного права і здійснюватися Генеральною Асамблеєю і Радою Безпеки (РБ), компетенція яких у цій сфері чітко розмежована. На Раду Безпеки ООН покладена головна відповідальність за підтримання міжнародного миру і безпеки. Відповідно до Статуту ООН, РБ володіє виключно широкими повноваженнями у справі попередження війни і створення умов щодо мирної і плідної співпраці країн. Підсумки діяльності Ради Безпеки можливо розглядати в якості критерію ефективності праці ООН (12).

Врятувати майбутні покоління від війни – таку мету поставили перед Організацією Об'єднаних Націй її засновники, які пережили руйнівні наслідки двох світових воєн. З моменту заснування організація працювала над тим, щоб запобігти переростанню конфлікту у війну, допомогти відновити мир у разі виникнення збройного конфлікту та допомогти зміцнити мир у тих регіонах, які пережили війну.

Таким чином, Рада Безпеки – єдиний орган Організації Об'єднаних Націй, який має повноваження вживати превентивних або примусових заходів від імені Організації Об'єднаних Націй. Відповідно до Статуту, Рада Безпеки відповідає за використання об'єднаних збройних сил держав-членів ООН.

Стаття 43 Статуту ООН визначає порядок надання членами ООН у розпорядження Ради Безпеки необхідних збройних сил, допоміжних засобів і обслуговування на підставі особливих угод, які укладаються РБ з державами-членами ООН при наступній їх ратифікації. РБ повинна вирішувати усі питання, пов'язані зі створенням і застосуванням збройних сил, спираючись на підтримку Воєнно-штабного комітету (ВШК), який складається з начальників штабів постійних членів Ради. Але положення статей 43 і 47 Статуту ООН не були введені в дію з причини розбіжностей серед постійних членів Ради Безпеки. У 1947 р. ВШК практично припинив свою діяльність. З тих пір в області створення і застосування збройних сил ООН стала імпровізувати. Саме за таких обставин виникла нова форма діяльності ООН щодо підтримання міжнародного миру і безпеки, яка не передбачена Статутом –миротворча (17).

Об'єднання зусиль держав для забезпечення та підтримки миру передбачає такі заходи, як заборона та загроза застосування сили в міждержавних відносинах, мирне вирішення міжнародних суперечок, підтримання безпеки, примусові заходи без використання збройних сил, примусові заходи з використанням збройних сил, роззброєння. Втім, розроблена система забезпечення миру у світі так і не спрацювала у повній мірі за весь час від закінчення Другої світової війни та від початку створення самої ООН та Ради Безпеки ООН відповідно. Відтак, виникає питання – чи виправдовує себе існування такої організації, наскільки ефективно вона виконує покладені на неї функції?

Рада Безпеки реагує на світові події різними способами — засудженням, встановленням фактів, процедурами підтвердження резолюцій і заяв Генеральної Асамблеї, рішеннями Генерального секретаря ООН тощо. Крім того, Рада Безпеки ООН має повноваження створювати миротворчі місії. Однак питання про ефективність цих методів залишається спірним і досі.

Миротворчі операції ООН розпочалися в 1948 році. Роль Місії Ради Безпеки на Близькому Сході полягала в моніторингу виконання угоди про перемир'я між державою Ізраїль і сусідніми арабськими державами. Пізніше операція була названа Організацією ООН з нагляду за

виконанням умов перемир'ям. Відтоді Організація Об'єднаних Націй розгорнула понад 70 миротворчих операцій. Миротворці залучаються за умов, коли Рада Безпеки ставила перед ООН завдання щодо дотримання режиму припинення вогню або розведення сил для підтримки міжнародного миру та безпеки, відповідно до положень Статуту Організації Об'єднаних Націй. Для підтримки міжнародного миру та безпеки миротворці не повинні відповідати вогнем на вогонь. Насамперед сили ООН здійснювали спостереження на місцях щодо дотримання режиму припинення вогню, виведення військ, створюючи усі умови для дипломатичних зусиль, які спрямовані на усунення основних причин конфлікту (4).

У цілому, операції Ради Безпеки були успішними. Так, у Сальвадорі і Мозамбіку миротворці ООН допомогли цим країнам пройти через перехідний період і надалі самостійно підтримувати мир. Втім, деякі зусилля зазнали невдачі. Наприклад, Рада Безпеки направляла миротворців у зони конфліктів, наприклад, до Сомалі та Боснії і Герцеговини, хоча там ще не було досягнуте припинення вогню і не було отримано згоди всіх сторін у конфлікті. Деякі мандати, надані цим місіям, виявилося неможливо виконати з тими ресурсами і персоналом, які були для цього надані. Крім того, у багатьох випадках держави-члени виявилися не готовими досягнути виконання власних рішень за допомогою примусу. Ці невдачі, найважливішими з яких стали масові вбивства в Сребрениці (Боснія і Герцеговина) 1995 р. і геноцид у Руанді 1994 р., змусили миротворців ООН ретельно проаналізувати концепцію операцій з підтримання миру.

Відтак, і до розгортання збройного конфлікту на території України унаслідок російської агресії Рада Безпеки ООН мала вагомі недоліки у своїй миротворчій діяльності. Зокрема, ООН не виробили механізму дій у випадках, якщо сторони конфлікту відмовлялися припиняти вогонь та порушували будь-які укладені мирні угоди. У таких випадках миротворці виявлялися безсилими й ООН ніяк не могло попередити чи зупинити війну та акти геноциду. Таким чином, Рада Безпеки ООН у багатьох випадках не справлялася зі своєю головною функцією щодо підтримки міжнародного миру та безпеки.

Війна російської федерації проти України порушує цілі та принципи, визначені в Статуті ООН з моменту його підписання в 1945 році. Війна має кілька фаз – це незаконна анексія Криму, збройний конфлікт на Донбасі (2014 – 2022 рр.) та повномасштабна війна росії проти України, яка почалася 24 лютого 2022 року. Відтак, найперші кроки Ради Безпеки ООН щодо попередження війни в Україні повинні були стосуватися саме анексії росією українського Криму у 2014 році. Втім, на цьому поприщі вказаний орган ООН не виявив жодної ефективності.

На думку І. Куса, експерта з міжнародної політики Українського інституту майбутнього, Рада Безпеки ООН не лише не змогла, а й взагалі не мала можливості запобігти анексії Криму, оскільки «дизайн» ООН взагалі не передбачав таких механізмів. 13 березня 2014 року Верховна

Рада України ухвалила Звернення до ООН, у якому зазначалося, що РФ намагається анексувати частину території України та вдасться до неспровокованого акту агресії. Вже тоді було очевидним, що дії Росії суперечать не тільки міжнародним нормам підтримання безпеки, але й дійсним двостороннім договорам, а також «духу і букві» міжнародних гарантій Україні, зафіксованих у Будапештському меморандумі (17).

У відповідь на це звернення ООН ініціювала обговорення питання та резолюцію щодо питання Криму в Україні, втім, попри те, що більшість членів Радбезу (13 країн) підтримало резолюцію, російська федерація, скориставшись правом вето, як постійний член Радбезу, фактично заблокувала рішення Ради Безпеки ООН щодо врегулювання української кризи.

Весь період боїв у зоні АТО, а пізніше ООС, Рада Безпеки ООН демонструвала такий же рівень ефективності – будь-які спроби цього органу сприяти урегулюванню військового конфлікту на території України блокувалися Росією. В той самий час, РФ навіть після масштабної військової агресії, геноциду українців, погроз всьому світу ядерною війною та визнання багатьма країнами Росії як країни-терористки, станом на 2022 рік все ще залишається членом ООН. Нездатність ООН навіть виключити росію зі складу країн-постійних членів вказує на надмірну бюрократизацію цієї організації та її неефективність у попередженні та врегулюванні конфліктів.

Ситуація не змінилася й станом на 2022 рік, адже протягом всього року, чинячи зухвалу військову агресію проти України, росія порушувала міжнародне право, неодноразово скликаючи Раду Безпеки ООН у спробах звинуватити в агресивних діях Україну. Відтак, надаючи майданчик для фейків, пропаганди та порушення норм міжнародного права терористичній державі росії, ООН та Рада Безпеки зокрема, втратили останню довіру до себе як до організацій, покликаних захищати мир у світі.

Не можна, втім, залишити без уваги ті спроби сприяти урегулюванню конфлікту, які Рада Безпеки все ж здійснює стосовно ситуації в Україні. Резолюції, дискусії та декларації ООН є важливими для фіксування історії, для міжнародного права, для країн-жертв агресії, оскільки при зміні політичної реальності є можливість апелювати до цих резолюцій в міжнародних судах.

У 2022 році РБ ООН неодноразово збирала засідання задля обговорення ситуації в Україні. У травні розглядалися проблеми захисту цивільного населення та інфраструктури в Україні в умовах російської агресії. В червні основна увага приділялася сексуальному насильству в контексті війни. Крім того, 28 червня відбулося окреме засідання через ракетний удар по місту Кременчуку, в результаті якого загинуло не менше 20 осіб.

Вирішення питання в Раді безпеки ООН незаконно блокується самою росією, яка не має права голосування по пов'язаному з нею питанню, однак робить це.

Окрім того, ООН достатньо ефективно реалізує свої повноваження у гуманітарних питаннях. Після нападу росії на Україну Організація Об'єднаних Націй розгорнула масштабну дільність з надання допомоги тим, хто був вимушено переміщений або постраждав від війни будь-яким іншим чином. Усього впродовж кількох тижнів мільйони людей втратили свої домівки та засоби існування у найшвидшій і найбільшій кризі переміщення населення за останній час.

Конфлікт охопив практично всі аспекти життя та діяльності людей – охорону здоров'я, культурну сферу, освіту, економічний розвиток, сільське господарство та інші, перетворивши деякі з процвітаючих і яскравих міст України на безлюдні та зруйновані міста-привиди. Він також закладає підвалини глобального дефіциту продовольства. Незважаючи на чимало ризиків та логістичні труднощі, низка агенств ООН разом з місцевими партнерами у короткому часовому проміжку змогли перемістили персонал з інших місій і встановили присутність у всіх адміністративних областях України, що вважається однією з найшвидших операцій з розширення, які коли-небудь проводила ООН.

Оскільки жертви серед цивільного населення зростали, сягаючи тисяч загиблих і поранених (з 24 лютого 2022 року внаслідок пов'язаного з конфліктом насильства в Україні щонайменше 10582 цивільні особи загинули, а 19875 було поранено (загальні втрати серед цивільних осіб – 30457 осіб) (рис. 4), агентства ООН максимально спрямували зусилля на допомогу постраждалим. У тому числі тим, хто опинився в облозі у Маріуполі, де ООН спільно з Міжнародним комітетом Червоного Хреста проводили місію з безпечного виїзду цивільних громадян.

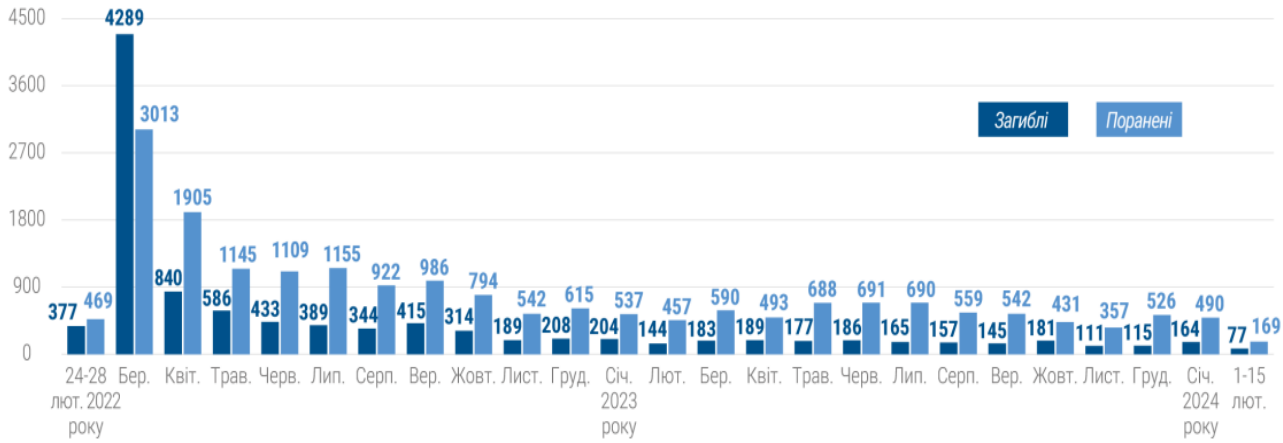


Рис. 4. Втрати серед цивільних осіб з 24 лютого 2022 року, по місяцях

Джерело: Дворічний звіт: Захист цивільних осіб вплив бойових дій на цивільних з 24 лютого 2022 року

Незважаючи на те, що бойові дії тривають, особливо на сході та півдні країни, ООН та український уряд, а також міжнародні донори та партнери розробляють плани щодо відновлення України. Швидка, жорстока та смертоносна війна показала неабияку мужність і стійкість українського народу перед обличчям лиха, а також безпрецедентну щедрість сусідніх держав, які відчинили свої двері для тих, хто залишили країну.

Однак, залишається фактом те, що Рада Безпеки ООН, як орган, головною задачею якого є підтримка міжнародного миру та безпеки в сучасному світі, з цією задачею не справляється, що особливо яскраво проявилося саме у ситуації війни росії проти України, яка стала найбільш масштабною війною у Європі у XXI столітті.

Таким чином, Рада Безпеки – колективний орган ООН, покликаний забезпечувати мир та безпеку у світі, однак який, на жаль, свою місію не виконує або ж виконує у недостатній мірі. Яскраво проявилося безсилля Радбезу ООН у ситуації збройної агресії росії проти України, яка почалася у 2014 році та не лише не стихла, однак вилилася у повномасштабну війну, яка загрожує перерости у міжнародний ядерний конфлікт.

Саме відсутність ефективних дій світової спільноти на чолі з ООН у відповідь на анексію росією українського Криму, збройну агресію та терористичні акти росії на українському Донбасі з 2014 р. підсилили впевненість цієї терористичної країни у її безкарності. Наслідком стала найбільша у Європі війна, відкритий геноцид українського народу зі сторони росіян, безліч жертв та руйнувань в Україні, а також вагома загроза безпеці країн-членів ООН, особливо – європейських країн. Станом на 2022 рік, який повністю пройшов під егідою злочинної війни та тероризму росії на континенті, ця країна й досі не виключена зі складу країн-членів ООН, що надає їй повноваження ветувати та блокувати будь-які рішення організації щодо забезпечення безпеки у світі.

Причини такої неефективності Ради Безпеки та ООН в цілому криються у недосконалому, бюрократизованому механізмі роботи цієї організації. У найближчому майбутньому ООН має або ж бути реформованим (і Україна вже розробила ініціативи з цього приводу), або ж цю організацію чекає доля Ліги Націй, яка припинила своє існування після Другої світової війни, оскільки не змогла запобігти цій війні, яка залишила половину Європи у руїнах.

Висновки

Міжнародні організації є специфічною формою прояву та організації співробітництва між різними країнами світу. У наш час багато країн стикаються з багатьма загрозами у сфері спільної політики безпеки та оборони, в тому числі із загрозою потенційних актів агресії на глобальному рівні. Безперечно, проблема забезпечення міжнародного правопорядку та глобальної безпеки є

однією з ключових у сучасних міжнародних відносинах і потребує нових підходів та нового рівня міждержавного співробітництва.

Варто підсумувати, що ні Ліга Націй, ні ООН не змогли повністю впоратися із завданням створення ефективної системи міжнародної безпеки. Час минає, а перманентна загроза глобальній безпеці залишається. Локальні війни спалахують із сумною регулярністю в усіх куточках земної кулі, в тому числі і в Європі. Початок XXI століття ознаменувався різким збільшенням політичних і військових конфліктів. Виникають історичні паралелі з жахливими подіями минулого століття. Саме тому сьогоднішня потреба у реформуванні існуючого світового порядку є цілком об'єктивною. Еволюція концепції міжнародної безпеки пройшла шлях від системи безпеки військового блоку до багатокомпонентної глобальної системи безпеки, яка включає різні підсистеми і функціонує на основі міжнародного права. Побудувати глобальну безпеку сьогодні дуже складно - занадто багато залежить від політичної волі держав. Таким чином, можна констатувати, що міжнародно-правове регулювання є невід'ємною частиною глобальної системи міжнародної безпеки. Наразі вже не можна стверджувати, що існуюча система нагляду за міжнародними відносинами є адекватною для XXI століття. Підвищення ефективності управління глобальними взаємодіями вимагає дій у трьох напрямках: упорядкування відносин між суверенними державами, модернізація існуючих багатосторонніх інститутів і створення ефективного наглядового органу.

Оцінено вплив та ефективність різних форм безпекового міжнародного співробітництва, що дозволило створити умовний рейтинг міжнародних безпекових організацій. Найбільш результативним за всіма параметрами є партнерство з НАТО. Відповідно, віддається помітна перевага спільним військовим навчанням, співробітництву в рамках операцій та місій, підготовці військових і цивільних фахівців у сфері безпеки саме з Альянсом – провідною політико-військовою організацією у світі.

Визначено, що найбільшою мірою відносинам України з ЄС і НАТО перешкоджає «російський фактор». Водночас, перешкодами співробітництву з ЄС є також низький рівень відповідальності української сторони за виконання взятих зобов’язань, інституційна слабкість України, брак компетентних кадрів і політичної волі. Співробітництву з НАТО перешкоджають, насамперед, такі чинники, як брак політичної волі та суспільної підтримки. Співробітництву з Митним союзом (МС) і ОДКБ заважають, першою чергою, розбіжності в цінностях, політичних цілях і стратегічних орієнтаціях.

Простежується недостатня результативність зовнішньої допомоги від міжнародних організацій в секторі безпеки і оборони та іноземних держав Україні у протистоянні російській агресії. Головні недоліки, а також причини такого стану справ детально висвітлені в документах

як міжнародного, так і національного рівня. Ключ до вирішення проблеми полягає в посиленні спільної відповідальності, гармонізації, узгодженні, орієнтації на результати і взаємній підзвітності донорів та отримувачів.

Зміцнення та вдосконалення системи глобальної безпеки в сучасному глобалізаційному світі вимагає не просто прийняття окремих нових міжнародно-правових норм, а розробки цілої серії міжнародно-правових актів у всіх сферах міжнародного співробітництва: військовій, економічній, екологічній, космічній, енергетичній, інформаційній тощо. При розробці цих міжнародних документів важливо враховувати універсальність проблем, регіональну специфіку, а також інтереси зацікавлених сторін у всій їх різноманітності та суперечливості. Необхідно також зміцнювати міжнародну інституційну базу для боротьби з новими викликами: створювати або реформувати експертні або міждержавні органи, комісії та комітети. Від того, наскільки ефективно і своєчасно це буде зроблено, залежить майбутнє людства.

References:

Офіційний сайт ОБСЄ. Режим доступу: https://www.osce.org/

Бехруз Х.Н., Андрейченко С.С., Грушко М.В. (2023). Міжнародне публічне право: основи теорії: підручник. Одеса: Юристика, 252 с.

Гулієв А.Д. Право міжнародних організацій: практичний посібник. Київ: Національний авіаційний університет, 2014. 64 с.

Гуменюк В. І. Організація з безпеки та співробітництва в Європі. Українська дипломатична енциклопедія: У 2-х т./Редкол.:Л. В. Губерський (голова) та ін. К.: Знання України, 2004 - Т.2 - 812с.

Денисов В.Н. Міжнародний правопорядок у світлі сучасних цивілізаційних викликів. Щорічник наукових праць «Правова держава», Київ, 2015, № 26, С. 391-401.

Джигора О.М., Кучменко В.О., Ковальчук В., Мельник В., Граб М. Вплив та ефективність діяльності міжнародних організацій на формування, забезпечення та зміцнення світового правопорядку. Журнал права та сталого розвитку, 2023. Маямі, №6. С. 01-25.

Європейська конвенція з прав людини (2021). Електронний ресурс. Режим доступу: https://zakon.rada.gov.ua/laws/show/995_004#Text

Індекс конфліктності ACLED. 2024. Електронний ресурс. Режим доступу: https://acleddata.com/conflict-index/

Козак Ю.Г., Ковалевський В.В., Логвінова Н.С. Міжнародні організації: Навчальний посібник. Київ: Центр навчальної літератури, 2009. 223 с.

Матвієнко В. Організація з безпеки та співробітництва в Європі. Політична енциклопедія. Редкол.: Ю. Левенець (голова) та ін. - К.: Парламентське видавництво, 2011. - С.516.

Женевський центр управління сектором безпеки (DCAF). Міжнародні організації. Режим доступу: https://securitysectorintegrity.com/uk

Патрік С. Реформа Ради Безпеки ООН: Що думає світ. Фонд Карнегі за міжнародний мир. 2023. Режим доступу: https://carnegieendowment.org/2023/06/28/

Пітерс, А. Міжнародні організації: Ефективність та підзвітність. Інститут порівняльного публічного права та міжнародного права імені Макса Планка (MPIL). 2016. Електронний ресурс. Режим доступу: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2770606

Рада Безпеки Організації Об'єднаних Націй (ООН). Безпека та врегулювання конфліктів у світі. Електронний ресурс. Режим доступу: http://lvivmun.sii.org.ua/security-council/
Рєзнікова О.О. Національна стійкість в умовах мінливого безпекового середовища: Монографія. Київ: Національний інститут стратегічних досліджень, 2022. 532 с.
Ринейська Л.С. Роль міжнародних організацій у формуванні міжнародних стратегій економічного розвитку. Електронний ресурс. Режим доступу: http://www.economy.nayka.com.ua/pdf/3_2018/56.pdf
Роль Ради Безпеки ООН у підтримці міжнародного миру та безпеки в сучасному світі та оцінка її ефективності на прикладі України. Електронний ресурс. Режим доступу: https://censs.org/rol-rady-bezpeky-oon-u-pidtrymtsi-mizhnarodnoho-myru-ta-bezpeky-v-suchasnomu-sviti-ta-otsinka-yiyi-efektyvnosti-na-prykladi-ukrayiny/
Саруші Д. Міжнародні організації та здійснення ними суверенних повноважень (Оксфордські монографії з міжнародного права). Видавництво Оксфордського університету. 2007.
Чайковський Ю. Держава і міжнародний правопорядок. Вісник НаУОА. Серія "Право", 2011. № 2(4), С. 1-12.
Чернега О.Б., Іваненко І.А. НАТО і система міжнародної безпеки: навчальний посібник для студентів вищих навчальних закладів. Донецький національний університет економіки і торгівлі імені Михайла Туган-Барановського. Донецьк: 2009, 228 с.
Шамраєва В.М. Основні теоретичні підходи до дослідження еволюції концепції міжнародної безпеки. Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм», 2008. № 8, С. 88- 94.

DOI 10.5281/zenodo.10820404
UDC 657:005.93

CHAPTER 5.
ACCOUNTING AND ANALYTICAL ENSURING ADMINISTRATION OF ADMINISTRATIVE DECISIONS

Maryna HALKEVYCH
Ph.D. in Economics, Associate Professor of Department of Business and Tourism Management,
Izmail University of Humanities
(12, Repin street, Izmail, Odesa region, 68600, Ukraine)
halkevych_maryna@ukr.net
https://orcid.org/0000-0002-4786-4856

Abstract. The article is devoted to the study of the issue of accounting and analytical support for management decision-making. The article defines the importance of the formation of effective systems of accounting, management accounting and analysis, as well as the interrelationships between them, which will contribute to increasing the effectiveness of accounting and analytical support for management decision-making. Some problems of regulatory and legal regulation of accounting support of management decisions are identified, including those related to the formation of the accounting policy of the enterprise. Peculiarities of management accounting in the system of accounting and analytical support for management decision-making have been studied. Including, the elements of accounting and management accounting, information needs of users at each stage of management decision-making are considered. The formation of a system of financial analysis at the enterprise as a basis for analytical support of management decision-making is considered. The classification of financial analysis, the sequence of financial analysis and the principles of financial analysis are given.

Keywords: accounting and analytical support for management decision-making, accounting, management accounting, financial analysis.

ОБЛІКОВО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ

Анотація. Стаття присвячена дослідженню питання обліково-аналітичного забезпечення прийняття управлінських рішень. У статті визначено важливість формування

ефективних систем бухгалтерського обліку, управлінського обліку та аналізу, а також взаємозв`язків між ними, що сприятиме підвищенню ефективності обліково-аналітичного забезпечення прийняття управлінських рішень. Визначено деякі проблеми нормативно-правового регулювання облікового забезпечення управлінських рішень, у тому числі, пов`язані із формуванням облікової політики підприємства. Досліджено особливості управлінського обліку у системі обліково-аналітичного забезпечення прийняття управлінських рішень. У тому числі, розглянуто елементи бухгалтерського та управлінського обліку, інформаційні потреби користувачів на кожному етапі прийняття управлінських рішень. Розглянуто формування системи фінансового аналізу на підприємстві як основи аналітичного забезпечення прийняття управлінських рішень. Наведена класифікація фінансового аналізу, послідовність проведення фінансового аналізу та принципи фінансового аналізу.

Ключові слова: обліково-аналітичне забезпечення прийняття управлінських рішень, бухгалтерський облік, управлінський облік, фінансовий аналіз.

Вступ. Найважливішою умовою функціонування та розвитку бізнес-сектору в будь-якій національній економіці є фінансово-економічна стабільність підприємств. Це зумовлено конкуренцією на зовнішньому та внутрішньому ринках. Фінансово-економічна стабільність підприємства базується на обліково-аналітичному забезпеченні, стан якого визначає ефективність і стійкість діяльності підприємства та створює передумови для подальшого розвитку за рахунок своєчасного виявлення та попередження зовнішніх і внутрішніх загроз і небезпек.

Постановка проблеми. Основою обліково-аналітичного забезпечення є інформація, тобто сукупність даних про внутрішнє та зовнішнє середовище підприємства, які використовуються для оцінки та аналізу господарських подій і процесів прийняття управлінських рішень.

Основними джерелами для оцінки та аналізу фінансового стану підприємства, фінансових результатів, ефективності використання фінансових ресурсів, кредитоспроможності та інвестиційної привабливості є фінансова звітність підприємства. Зокрема, баланс є основою для аналізу фінансового стану підприємства, а звіт про фінансові результати дозволяє проаналізувати структуру доходів і витрат підприємства і визначити основні фінансові результати його діяльності – прибуток.

Фінансова звітність є важливим інструментом для управління фінансовими процесами та явищами компанії. Основною базою для проведення фінансового аналізу в бізнесі є

результати бухгалтерського обліку, які являють собою безперервний єдиний процес обліку господарських операцій в залежності від стану власності та зобов'язань підприємства. Точність і ясність фінансової звітності є передумовами для ефективного фінансового аналізу та оптимізації управлінських рішень.

Разом з тим, варто зазначити, що фінансова звітність не може задовольнити всі інформаційні потреби внутрішніх користувачів інформації. Відповідно, на підприємстві з метою надання своєчасної та повної інформації менеджерами для прийняття рішень доцільно сформувати систему управлінського обліку, який, хоч і будується на даних господарського обліку, але має свої особливі цілі та завдання, власні методи, періодичність та елементи звітності.

Аналіз останніх досліджень і публікацій. Різні аспекти обліково-аналітичного забезпечення прийняття управлінських рішень широко досліджено у наукових працях. Зокрема, такими авторами як С. Ф. Голов, В. І. *(Голов С., 2017)*, М. Г. Чумаченко *(Чумаченко М., 2003)*, Т. В. Косташ, М. Р. Смола *(Косташ Т., Смола М., 2021)*, В. В. Биба, Ю. І. Матюшина *(Биба В., Матюшина Ю., 2015),* З.-М. В. Задорожний, Я. Ф. Аверкин *(Задорожний З.-М., Аверкин Я., 2017)* були досліджені проблеми бухгалтерського та управлінського обліку, їх ролі в інформаційному забезпеченні управління підприємством, сутність завдання та етапи впровадження системи управлінського обліку тощо. Разом з тим, дослідження проблем обліково-аналітичного забезпечення прийняття управлінських рішень не є вичерпною, оскільки формування на підприємстві ефективної системи обліково-аналітичного забезпечення прийняття управлінських рішень передбачає побудову систем бухгалтерського та управлінського обліку, системи фінансово-економічного аналізу на підприємстві, а також їх взаємозв`язків.

1.Проблеми нормативно-правового регулювання облікового забезпечення прийняття управлінських рішень

Бухгалтерський облік є процесом реєстрації, узагальнення, зберігання та передачі інформації про фінансово-господарську діяльність підприємства внутрішнім та зовнішнім користувачам для прийняття управлінських рішень. Важливість формування ефективної системи бухгалтерського та управлінського обліку обумовлена тим, що бухгалтерський облік є одним з основних джерел інформації про фінансово-господарську діяльність підприємств та організацій, а тому від ефективності організації бухгалтерського обліку залежить ефективність діяльності підприємства. Разом з тим, ефективність бухгалтерського обліку, у свою чергу, залежить від досконалості системи його нормативно-правового регулювання.

Нормативно-правова база бухгалтерського обліку - це сукупність законів і нормативних актів, що регулюють фінансово-господарську діяльність підприємств та ведення бухгалтерського обліку і складання фінансової звітності.

Система регулювання бухгалтерського обліку в Україні складається з чотирьох рівнів: міжнародні норми, державні норми, положення (стандарти) бухгалтерського обліку та інструкції щодо їх застосування, методичні рекомендації з бухгалтерського обліку та внутрішні нормативні документи підприємств з питань регулювання бухгалтерського обліку (рис. 1).

Міжнародні норми регулювання обліку включають міжнародні стандарти фінансової звітності, міжнародні стандарти бухгалтерського обліку та концептуальну основу складання та подання фінансової звітності.

Міжнародні стандарти фінансової звітності та міжнародні стандарти бухгалтерського обліку - це сукупність нормативних документів, які визначають загальні правила складання фінансової звітності та порядок відображення інформації про об'єкти обліку у фінансовій звітності суб'єкта господарювання.

Рис. 1. Система нормативно-правового регулювання бухгалтерського обліку в Україні

Побудовано автором

Міжнародні стандарти бухгалтерського обліку та Міжнародні стандарти фінансової звітності рекомендовані на міжнародному рівні. Закон України "Про бухгалтерський облік та

фінансову звітність" визначає, що ті підприємства, які становлять суспільний інтерес, зобов'язані для складання фінансової звітності застосовувати Міжнародні стандарти бухгалтерського обліку та звітності, всі інші підприємства мають право самостійного вибору концептуальної основи складання та подання фінансової звітності *(Закон України «Про бухгалтерський облік та фінансову звітність в Україні, 1999)*.

Державні норми регулювання обліку в Україні включають Закон України «Про бухгалтерський облік та фінансову звітність в Україні», Господарський кодекс України та Податковий кодекс України.

Основним нормативним документом, що регулює бухгалтерський облік в Україні, є Закон України "Про бухгалтерський облік та фінансову звітність в Україні", яким встановлюється особливості державного регулювання бухгалтерського обліку та фінансової звітності в Україні, вимоги до організації та ведення бухгалтерського обліку, складання та подання фінансової звітності. Закон також встановлює принципи бухгалтерського обліку, які є загальними та основними вимогами до інформації, що має бути представлена в бухгалтерському обліку та фінансовій звітності підприємства відповідно до міжнародних стандартів бухгалтерського обліку та національних положень (стандартів) бухгалтерського обліку: повне висвітлення, автономність, єдиний грошовий вимірник, безперервність, нарахування, превалювання сутності над формою, послідовність та інші принципи *(Закон України «Про бухгалтерський облік та фінансову звітність в Україні, 1999)*.

Наведені принципи у МСБО та у Законі України «Про бухгалтерський облік та фінансову звітність в Україні» мають певні відмінності (таблиця 1).

Таблиця 1

Принципи бухгалтерського обліку за МСБО та Законі України «Про бухгалтерський облік та фінансову звітність в Україні»

Закон України «Про бухгалтерський облік та фінансову звітність в Україні»	МСБО 1 «Подання фінансової звітності»	Зміст
Повного висвітлення	-	Вимагає розкриття всієї важливої для прийняття управлінських рішень інформації про діяльність підприємства
Автономності	-	Майно та зобов`язання підприємства необхідно відокремлювати від майна та зобов`язань власників даного підприємства
Єдиного грошового вимірника	-	Фінансова звітність підприємств України складається у тисячах гривнях

Безперервність	Безперервність	Оцінку активів та зобов`язань доцільно здійснювати на підставі припущення, що діяльність підприємства триватиме у подальшому
Нарахування	Нарахування	Фінансовий результат діяльності підприємства визначається шляхом співставлення доходів та витрат, що були понесені для отримання доходів звітного періоду
Превалювання сутності над формою	-	Операції у фінансовій звітності відображуються за їх економічним змістом, а не юридичною сутністю
	Суттєвість та об`єднання у групи	Кожний суттєвий клас статей подається окремо, але несуттєві рядки фінансової звітності можливо об`єднати у групи
Послідовності	Послідовність подання	Застосування обраної облікової політики, що була розроблена
-	Частота звітності	Мінімальний пакет звітності необхідно подавати щонайменше щороку
-	Згортання	Передбачає недопущення згортання активів, зобов`язань, доходів та витрат
-	Порівняльна інформація	Щодо кожної статті у фінансовій звітності необхідно наводити інформацію попередніх періодів

Побудовано автором

Крім того, Національним положенням (стандартом) бухгалтерського обліку 1 «Загальні вимоги до фінансової звітності» визначені такі принципи, як:

- обачності, який вимагає недопущення завищення оцінки активів та заниження оцінки зобов`язань;

- історичної (фактичної) собівартості, відповідно до якого оцінка активів здійснюється, виходячи з витрат на їх виробництво;

- періодичності, за яким вся діяльність підприємства умово поділяється на періоди для складання фінансової звітності *(НП(С)БО 1 «Загальні вимоги до фінансової звітності», 2013).*

Отже, за даними таблиці видно, що принципи бухгалтерського обліку за міжнародними та національними нормами мають певні відмінності, а саме:

- у міжнародних нормах відсутні такі принципи, як повного висвітлення, єдиного грошового вимірника, автономності, превалювання сутності над формою;

- у національних нормах відсутні принципи: суттєвість та об`єднання у груп и, частота звітності, згортання, порівняльна інформація.

Як наслідок, основні вимоги до бухгалтерського обліку та фінансової звітності за державними та міжнародними нормами не гармонізовані. Наявність неузгоджених питань між міжнародними та національними нормами бухгалтерського обліку може призвести до того, що інформація, сформована у фінансовій звітності може бути не зрозумілими зовнішнім користувачам фінансової звітності – вітчизняним або закордонним.

Господарський кодекс України регламентує господарську діяльність підприємств з метою забезпечення розвитку підприємництва в Україні, зростання ефективності суспільного виробництва та підвищення ділової активності вітчизняних підприємств. Статтею 18 Господарського кодексу України визначена вимога до всіх суб'єктів господарської діяльності, а також структурних підрозділів підприємств, які виділені на окремий баланс, щодо ведення первинного (оперативного) обліку господарської діяльності, складання та подання відповідно до чинного статистичної та іншої інформації, ведення бухгалтерського обліку та подання фінансової звітності *(Господарський кодекс України, 2003).*

Податковий кодекс України регламентує порядок оподаткування підприємств, а також особливості обліку господарських операцій з метою їх правильного оподаткування, нарахування та сплати податків, а також складання та подання податкової звітності *(Податковий кодекс України, 2010).*

Третій рівень нормативно-правового забезпечення обліку на підприємстві включає Національні положення (стандарти) бухгалтерського обліку, План рахунків бухгалтерського обліку, Інструкція до застосування Плану рахунків бухгалтерського обліку.

Національні положення (стандарти) бухгалтерського обліку, як і Міжнародні стандарти фінансової звітності, є сукупністю нормативних документів, що визначають порядок відображення інформації про об'єкти бухгалтерського обліку (господарські засоби та джерела їх утворення, господарські процеси) на рахунках бухгалтерського обліку та у фінансовій звітності. Національними положеннями (стандартами) бухгалтерського обліку регламентуються такі питання обліку (таблиця 2).

Таблиця 2

Питання бухгалтерського обліку та фінансової звітності, які регулюються Національними положеннями (стандартами) бухгалтерського обліку

Питання бухгалтерського обліку та фінансової звітності	НПС(Б)О

1.Вимоги до складання та подання фінансової звітності	НП(С)БО 1 «Загальні вимоги до фінансової звітності» НП(С)БО 2 «Консолідована фінансова звітність» НП(С)БО 6 «Виправлення помилок і зміни у фінансових звітах» НП(С)БО 23 «Розкриття інформації щодо пов`язаних сторін» НП(С)БО 25 «Спрощена фінансова звітність» НП(С)БО 29 «Фінансова звітність за сегментами»
2.Облікова політика підприємства	НП(С)БО 6 «Виправлення помилок і зміни у фінансових звітах»
3.Відображення в обліку та звітності інформації про необоротні активи	НП(С)БО 7 «Основні засоби» НП(С)БО 8 «Нематеріальні активи» НП(С)БО 27 «Необоротні активи, утримувані для продажу, та припинена діяльність» НП(С)БО 28 «Зменшення корисності активів» НП(С)БО 30 «Біологічні активи» НП(С)БО 32 «Інвестиційна нерухомість» НП(С)БО 33 «Витрати на розвідку корисних копалин»
4. Відображення в обліку та звітності інформації про запаси	НП(С)БО 9 «Запаси» НП(С)БО 30 «Біологічні активи»
5. Відображення в обліку та звітності інформації про розрахунки з дебіторами та кредиторами	НП(С)БО 10 «Дебіторська заборгованість» НП(С)БО 11 «Зобов`язання» НП(С)БО 34 «Платіж на основі акцій»
6. Відображення в обліку та звітності інформації про інвестиційну діяльність	НП(С)БО 12 «Фінансові інвестиції» НП(С)БО 13 «Фінансові інструменти»
7. Відображення в обліку та звітності інформації про орендні операції	НП(С)БО 14 «Оренда»
8. Відображення в обліку та звітності інформації про фінансові результати діяльності підприємства	НП(С)БО 15 «Дохід» НП(С)БО 16 «Витрати» НП(С)БО 17 «Податок на прибуток» НП(С)БО 24 «Прибуток на акцію» НП(С)БО 31 «Фінансові витрати»
9. Відображення в обліку та звітності інформації про будівельні контракти	НП(С)БО 18 «Будівельні контракти»
10. Відображення в обліку та звітності інформації про об`єднання підприємств	НП(С)БО 19 «Об`єднання підприємств»

11. Відображення в обліку та звітності інформації про інфляцію та зміну валютних курсів	НП(С)БО 21 «Вплив змін валютних курсів» НП(С)БО 22 «Вплив інфляції»
12. Відображення в обліку та звітності інформації про виплати працівникам	НП(С)БО 26 «Виплати працівникам»

Побудовано автором

На рівні підприємства бухгалтерський облік регулюється внутрішніми правилами: наприклад, "Наказом про облікову політику" та "Правилами ведення бухгалтерського обліку". Внутрішні правила не повинні суперечити державним нормативним актам з бухгалтерського обліку. Проте в Україні недостатньо врегульовано порядок розробки облікової політики, її зміст, впровадження наказів про облікову політику та внесення змін до них *(Лист Міністерства фінансів України «Про облікову політику», 2005)*.

Нормативними документами з питань регулювання облікової політики є:

1. Закон України "Про бухгалтерський облік та фінансову звітність в Україні", який визначає поняття "облікова політика" як сукупність принципів, методів і процедур, що використовуються підприємством для складання та подання фінансової звітності *(Закон України «Про бухгалтерський облік та фінансову звітність в Україні», 1999).*

2. Лист Міністерства фінансів України "Про облікову політику" від 21 грудня 2005 року містить неповний перелік загальних положень та елементів облікової політики *(Лист Міністерства фінансів України «Про облікову політику», 2005).*

3. Лист Міністерства фінансів України "Про облікову політику" від 14 травня 2012 року роз'яснюється поняття облікових оцінок та зазначаються обставини, які можуть призвести до перегляду облікових оцінок (зокрема, зміна обставин, на яких ґрунтується облікова оцінка, або отримання додаткової інформації), зміни в облікових оцінках та обліковій політиці *(Лист Міністерства фінансів України «Про облікову політику», 2012).*

4) НП(С)БО 6 «Виправлення помилок і зміни у фінансових звітах» встановлює порядок визнання помилок і змін в облікових оцінках у фінансовій звітності *(НП(С)БО 6 «Виправлення помилок і зміни у фінансових звітах», 1999)*.

Отже, законодавством не визначено зміст складових облікової політики, повний перелік її елементів, процедури формування, затвердження та внесення змін до наказів про облікову політику, які, до речі, є основними внутрішніми розпорядчими документами з питань бухгалтерського обліку та фінансової звітності.

Таким чином, система нормативно-правового регулювання бухгалтерського обліку в Україні включає чотири рівні, спрямовані на забезпечення реалізації основної мети

бухгалтерського обліку - надання користувачам повної, правдивої та неупередженої інформації. Водночас недоліки, що існують у нормативно-правовій системі бухгалтерського обліку, ускладнюють ведення бухгалтерського обліку та складання фінансової звітності. Серед недоліків нормативно-правового регулювання бухгалтерського обліку в Україні можна виділити, зокрема, такі: розбіжності в принципах ведення бухгалтерського обліку та складання фінансової звітності між національними положеннями (стандартами) бухгалтерського обліку та міжнародними стандартами фінансової звітності, хоча вітчизняним підприємствам дозволено застосовувати міжнародні стандарти фінансової звітності. Крім того, законодавством не визначено зміст складових облікової політики, повний перелік її елементів, процедури формування, затвердження та внесення змін до наказів про облікову політику тощо. Виявлені недоліки нормативно-правового регулювання облікового забезпечення прийняття управлінських рішень можуть спричинити зниження якості інформації, що формуються у системі бухгалтерського обліку. З метою підвищення якості бухгалтерського обліку українських підприємств та інформації, що надається у фінансовій звітності, необхідно оптимізувати систему нормативно-правового регулювання бухгалтерського обліку.

2. Управлінський облік у системі обліково-аналітичного забезпечення прийняття управлінських рішень

Діяльність будь-якого підприємства пов'язана з ефективністю, точністю та своєчасністю прийняття управлінських рішень, які залежать від якості та оперативності інформації про фінансово-господарську діяльність підприємства. Основним джерелом інформації на підприємстві є система бухгалтерського обліку, яка призначена для широкого кола внутрішніх і зовнішніх користувачів. Натомість управлінський облік орієнтований на внутрішніх користувачів інформації, і хоча він не є обов'язковим на підприємствах, ефективна система управлінського обліку забезпечує керівництво оперативною інформацією, необхідною для своєчасного прийняття рішень. Сьогодні багато вітчизняних підприємств впроваджують системи обліку, орієнтовані на виконання вимог законодавства, особливо у сфері оподаткування, і зовсім не впроваджують систему управлінського обліку. Тому необхідним є дослідження особливостей та практичної значущості систем бухгалтерського та управлінського обліку як інформаційної підтримки в процесі прийняття управлінських рішень.

Бухгалтерський облік на вітчизняних підприємствах регулюється законодавчо. Відповідно до Закону України "Про бухгалтерський облік та фінансову звітність в Україні" бухгалтерський облік є процесом виявлення, вимірювання, реєстрації, узагальнення, накопичення, зберігання та передачі інформації про діяльність підприємства внутрішнім та

зовнішнім користувачам *(Закон України «Про бухгалтерський облік та фінансову звітність в Україні», 1999)*. Усі підприємства зобов'язані вести бухгалтерський облік, пов'язаний з їх господарською діяльністю.

Управлінський облік не передбачений чинним законодавством і немає обов'язку вести управлінський облік. Не існує єдиного розуміння поняття управлінського обліку. Зокрема, С.Ф. Голов та В.І. Єфименко визначають управлінський облік як процес виявлення, вимірювання, накопичення, узагальнення, аналізу, інтерпретації та передачі інформації керівництву з метою виконання управлінських функцій *(Голов С., Єфименко В., 1996)*. На думку М. Г. Чумаченка, управлінський облік є результатом цілеспрямованого розвитку всього бухгалтерського обліку для забезпечення інформацією, що відповідає потребам управління *(Чумаченко М., 2003)*. Автори Т.В. Косташ та М.Р. Смола стверджують, що управлінський облік є чимось більшим, ніж система бухгалтерського обліку, і призначений для задоволення інформаційних потреб керівництва для виконання управлінських функцій, таких як планування, організація, мотивація та контроль *(Косташ М., Смола М., 2021)*. Т.В. Косташ та А.Г. Карп також відрізняють управлінський облік від фінансового, але визначають управлінський облік як найважливішу частину єдиного інформаційного простору, базу знань та сукупність інформаційних ресурсів підприємства *(Косташ Т., Карп А., 2021)*.

Таким чином, науковці загалом сходяться на думці, що управлінський облік спрямований на задоволення інформаційних потреб менеджерів для виконання ними своїх функцій. На основі проведеного дослідження можна зробити висновок, що управлінський облік - це система на підприємстві, організована в інтересах його власників для реєстрації, накопичення, узагальнення та передачі інформації про фінансово-господарську діяльність, доходи і витрати підприємства та його сегментів з метою надання керівництву можливості виконувати свої управлінські функції. Можна зробити висновок, що бухгалтерський та управлінський облік - це різні системи, які базуються на даних господарського обліку підприємства, але мають власні цілі, завдання, суб'єкти, об'єкти, методи, джерела вхідної інформації та результати функціонування на виході системи (табл. 3).

Таблиця 3.

Елементи систем бухгалтерського обліку та управлінського обліку

Елемент	Бухгалтерський облік	Управлінський облік
Ціль	Метою бухгалтерського обліку є формування правдивої, повної та неупередженої інформації про фінансові результати діяльності та фінансовий стан підприємства	Метою управлінського обліку є формування неупередженої, повної та правдивої інформації про фінансово-господарські результати діяльності підприємства, окремих його напрямів

	та її передачі користувачам як внутрішнім, так і зовнішнім для прийняття управлінських рішень	діяльності та підрозділів та її передачі внутрішнім користувачам з метою забезпечення реалізації ними функцій управління
Завдання	- формування правдивої і повної інформації про активи, пасиви та фінансові результати діяльності підприємств; - забезпечення контролю за ефективністю використання ресурсів підприємства та його активами; - забезпечення контролю розрахунків підприємства з його кредиторами та дебіторами	-надання управлінському персоналу оперативної інформації для прийняття ними рішень; -забезпечення контролю за витратами підприємства за рахунок їх обліку за центрами відповідальності та за видами; -планування бюджету та здійснення контролю за його виконанням; -ведення оперативного обліку розрахунків із контрагентами з метою підвищення ефективності використання фінансових ресурсів
Об`єкт	- активи підприємства та джерела їх формування; - господарські процеси на підприємстві: процес постачання, процес виробництва та процес реалізації	- результати господарської діяльності підприємства і його підрозділів; - бюджети підприємства і його підрозділів; - витрати підприємства за видами діяльності, за елементами тощо і його підрозділів; -процес ціноутворення.
Суб`єкт	Підприємство (організація)	Управлінський персонал підприємства
Предмет	Вся фінансово-господарська діяльність підприємства	Виробнича діяльність підприємства в цілому і його підрозділів
Методи	Методами, які застосовуються в бухгалтерському обліку є такі, як інвентаризація, документування, калькуляція, оцінка, рахунок та подвійний запис, баланс, інші форми фінансової звітності	Методи управлінського обліку класифікуються за такими критеріями: -об`єкта обліку; -напрям застосування; -термін даних; -повнота включення витрат у собівартість; -собівартість.
Звітність	Фінансова бухгалтерська звітність підприємства, яка є ретроспективною. Фінансова звітність підприємств не є конфеденційною	Управлінська звітність, яка має перспективне спрямування та є конфеденційною

Побудовано автором

Таким чином, метою систем бухгалтерського та управлінського обліку є надання повної, правдивої та неупередженої інформації для прийняття управлінських рішень, але бухгалтерський облік призначений як для зовнішніх, так і для внутрішніх користувачів, тоді

як управлінський облік призначений лише для внутрішніх користувачів. Управлінський облік також відрізняється від бухгалтерського тим, що надає інформацію не тільки про бізнес в цілому, але й про окремі підрозділи, напрямки діяльності тощо.

Завдання систем бухгалтерського та управлінського обліку також відрізняються: якщо основним завданням бухгалтерського обліку є управління збереженням цінностей, своєчасністю розрахунків та формування достовірної інформації про фінансово-господарську діяльність підприємства, то основним завданням управлінського обліку є забезпечення керівництва інформацією для прийняття господарських рішень та надання їм цієї інформації для досягнення стратегічних цілей підприємства *(Чумаченко М., 2003).*

Об'єктом системи бухгалтерського обліку є самостійна господарська одиниця (підприємство), відокремлена від інших господарських одиниць, що має власні активи та джерела їх формування. Суб'єктом системи управлінського обліку є господарська одиниця (підприємство) в особі менеджерів різних рівнів.

Об'єктами системи бухгалтерського обліку є господарські засоби та джерела їх утворення (активи і зобов'язання) і господарські процеси (закупівля, виробництво, реалізація), а системи управлінського обліку - результати діяльності підприємства та його окремих підрозділів, витрати підприємства та його окремих підрозділів, бюджети і ціноутворення підприємства та його окремих підрозділів *(Косташ Т., Смола М., 2021)*.

Суб'єктом системи бухгалтерського обліку є господарська діяльність підприємства; система управлінського обліку управляє виробничою діяльністю підприємства в цілому та окремо за підрозділами, сферами діяльності тощо.

Системи бухгалтерського обліку використовують елементи методів бухгалтерського обліку, такі як документація, інвентаризація, оцінка, калькуляція, рахунки, подвійний запис, бухгалтерські баланси та інші форми звітності. Методи системи управлінського обліку класифікуються за кількома критеріями, зокрема напрям застосування (фінансові, економічні, статистичні, кібернетичні, системні), об'єкт обліку (за центрами витрат, за видами витрат, за розподілом витрат, за місцями виникнення витрат), повнота витрат, що включаються до собівартості (повна виробнича собівартість, обмежена виробнича собівартість), період даних (історичні дані, поточні дані, майбутні дані); собівартість (стандарт-костінг, директ-костінг).

Система бухгалтерського обліку формує фінансову звітність, включаючи баланс, звіти про сукупний дохід (звіт про фінансові результати), звіт про рух грошових коштів, звіт про власноий капітал та примітки до фінансової звітності. Бухгалтерська (фінансова) звітність є ретроспективною і не завжди надає своєчасну інформацію для прийняття своєчасних управлінських рішень. Бухгалтерська (фінансова) звітність призначена як для внутрішніх, так

і для зовнішніх користувачів і підлягає оприлюдненню. Результатом системи управлінського обліку є управлінська звітність, яка, на відміну від бухгалтерської (фінансової) звітності, є конфіденційною та оперативною, хоча і не регулюється законодавчо.

Таким чином, системи бухгалтерського та управлінського обліку спрямовані на надання користувачам повної, правдивої та неупередженої інформації для прийняття управлінських рішень. Однак вони спрямовані на вирішення різних інформаційних завдань в управлінській діяльності, оскільки орієнтовані на різну аудиторію і використовуються по-різному.

Процес прийняття управлінських рішень включає такі етапи: визначення та аналіз проблеми, постановка цілей, визначення альтернатив, оцінка альтернатив та вибір найкращої альтернативи, прийняття управлінського рішення та управління. Кожен з цих етапів потребує відповідної інформації (табл. 4).

Таблиця 4

Інформаційні потреби на кожному етапі прийняття управлінського рішення

Етап прийняття управлінського рішення	Дані систем бухгалтерського та управлінського обліку
1.Виявлення проблеми та її аналіз	-інформація про фінансовий стан підприємства та фінансові результати його діяльності, наведена у фінансовій звітності; -інформація, наведена в управлінській оперативній звітності в цілому по підприємству, а також за окремими його підрозділами, напрямами діяльності тощо; -планова інформація та інформація, наведена в бюджетах, виявлення відхилень між плановими та фактичними показниками
2.Встановлення цілей	Формування планової інформації
3.Визначення можливих альтернатив	Прогнозні дані про фінансово-господарську діяльність підприємства у цілому та за окремими підрозділами або напрямами діяльності
4.Оцінка та вибір альтернатив	Фінансово-економічне обґрунтування вибору найбільш оптимальної альтернативи
5.Прийняття управлінського рішення та контроль	Систематичне співставлення прогнозних (планових) та фактичних даних, у тому числі на підставі оперативних звітів

Побудовано автором

Таким чином, системи бухгалтерського та управлінського обліку є інформаційною інфраструктурою, що підтримує управлінську діяльність. Хоча бухгалтерський облік є обов'язковим для всіх підприємств, його організація на підприємстві повинна враховувати не тільки інформаційні потреби зовнішніх користувачів інформації (забезпечення дотримання

вимог законодавства), а й потреби внутрішніх користувачів (менеджерів, які задовольняють свої інформаційні потреби для прийняття управлінських рішень). Управлінський облік не є обов'язковим для бізнесу, але цілі, методи і завдання системи управлінського обліку, а отже, і звітність, що формується в результаті її функціонування, відрізняються від цілей, методів і завдань системи бухгалтерського обліку. Таким чином, бухгалтерський облік сам по собі, хоча і є основним джерелом інформації про фінансово-господарську діяльність підприємства, не може повністю задовольнити інформаційні потреби керівництва для прийняття своєчасних та ефективних управлінських рішень.

3.Формування системи фінансового аналізу на підприємстві як основи аналітичного забезпечення прийняття управлінських рішень

Здійснення ефективної підприємницької діяльності в умовах ринкової економіки базується на створенні сучасних систем інформаційно-аналітичної підтримки управління фінансово-господарською діяльністю. Його складовими є облік, аналіз, управління фінансово-господарськими операціями, процесами та явищами.

Фінансовий аналіз є сукупністю методичних прийомів, що використовуються для дослідження фінансових відносин суб'єктів господарювання. Фінансові відносини підприємства зумовлені об'єктивними та суб'єктивними факторами, які відображаються у фінансовому обліку та звітності.

Пріоритетним напрямком фінансового аналізу є дослідження формування, розподілу та використання фінансових ресурсів як основного виду ресурсів підприємства.

Фінансовий аналіз - це процес дослідження фінансового стану підприємства та результатів його фінансової діяльності з метою виявлення резервів підвищення ринкової вартості підприємства та забезпечення його ефективного розвитку. Також фінансовий аналіз визначається, як сукупність спеціальних знань, спрямованих на вивчення фінансових відносин, фінансових ресурсів і причинно-наслідкових зв'язків у їхньому русі з метою оцінки життєвого стану та перспектив розвитку підприємства.

Класифікація фінансового аналізу наведена на рис. 2.

Залежно від суб'єкта дослідження розрізняють внутрішній та зовнішній фінансовий аналіз. Суб'єктами внутрішнього аналізу є керівники структурних підрозділів та центрів відповідальності компанії, бухгалтерські та фінансові служби, центри управління персоналом та інший персонал, до функціональних обов'язків якого входять функції управління та аналізу.

Зовнішній фінансовий аналіз здійснюється сторонніми аналітиками, аудиторами, фахівцями з оцінки, фінансовими установами, інвесторами, кредиторами, постачальниками, клієнтами, комерційними банками та консалтинговими компаніями.

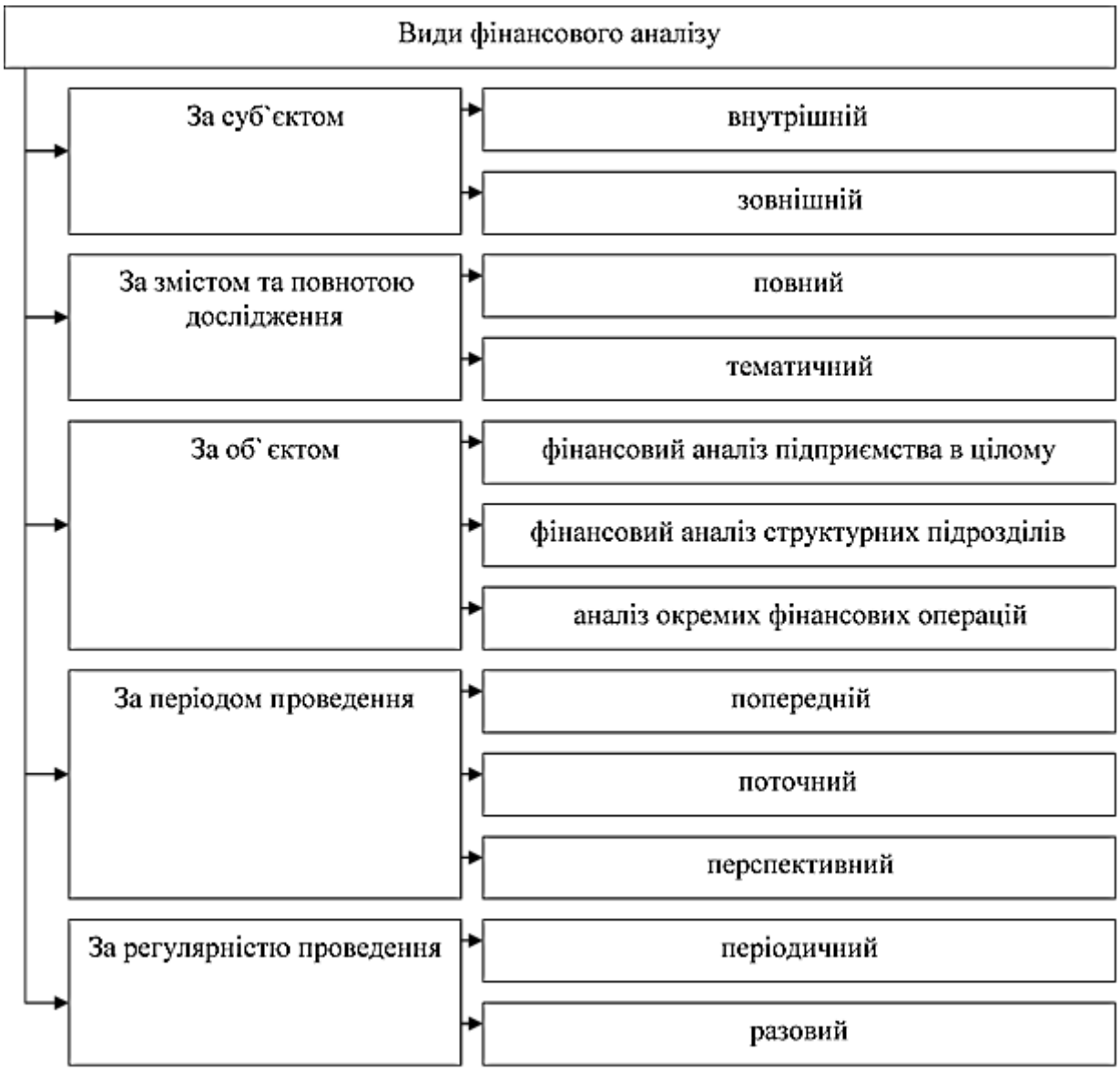


Рис. 2. Класифікація фінансового аналізу

Побудовано автором

До особливостей зовнішнього фінансового аналізу можна віднести:

- численні аналітичні аудиторії, користувачі інформації про діяльність організації;
- різноманітність цілей та інтересів аналітичної аудиторії;
- наявність стандартизованих методик, стандартів обліку та звітності;
- аналіз фокусується виключно на офіційній зовнішній звітності компанії;
- обмеженість роботи аналітика внаслідок дії вищезазначених факторів;
- максимальне розкриття результатів аналізу користувачам інформації про діяльність компанії.

До особливостей внутрішнього фінансового аналізу можна віднести:

- вузьку сферу аналізу;

- максимальне конфіденційне розкриття результатів аналізу внутрішнім користувачам (як правило, керівництву компанії), результати такого аналізу можуть становити комерційну таємницю;

- використання всіх доступних джерел інформації, включаючи використання даних фінансового та управлінського обліку, для проведення змістовного та глибокого фінансового аналізу;

- застосування нерегламентованих методів аналітичних досліджень на додаток до стандартних аналітичних методів;

-проводення більш поглибленої аналітичної роботи для прийняття відповідних управлінських рішень;

-здійснення необхідного аналізу відповідно до потреб управління.

Повний фінансовий аналіз здійснюється шляхом вивчення всіх аспектів фінансової складової діяльності підприємства на підприємстві. Відповідно, аналізуються всі аспекти фінансової складової діяльності підприємства і за результатами готується комплексний аналітичний звіт.

Тематичний фінансовий аналіз обмежується дослідженням окремих аспектів фінансової складової діяльності підприємства.

До напрямів тематичного фінансового аналізу відносяться:

1) Ефективність використання активів;

2) Оптимізація фінансування різних активів з окремих джерел;

3) Фінансова стійкість і платоспроможність;

4) Оборотність і якість дебіторської заборгованості;

5) Прибутковість виробництва (продажу) окремих товарів;

6) Оптимальність інвестиційного портфеля.

Залежно від характеру предмета аналізу розрізняють такі види фінансового аналізу:

1) Аналіз фінансової діяльності підприємства в цілому;

2) Аналіз фінансової діяльності окремих структурних підрозділів та відділів;

3) Аналіз окремих фінансових операцій;

4) Аналіз фінансової діяльності організації в цілому.

Аналіз фінансової діяльності окремих структурних одиниць та підрозділів переважно базується на результатах управлінського обліку організації і спрямований на аналіз центрів економічної відповідальності. Наприклад, оцінюється ефективність фінансової діяльності філій, відділень, представництв, виробничих і складських підрозділів, транспортних одиниць тощо.

Об'єктом такого аналізу окремих фінансових операцій є окремі операції, пов'язані з короткостроковими або довгостроковими фінансовими вкладеннями, фінансуванням окремих реальних проектів, оцінкою ефективності використання банківських кредитів, оцінкою економічної доцільності модернізації обладнання тощо.

Попередній фінансовий аналіз - це дослідження стану фінансових складових діяльності в цілому або здійснення окремих фінансових операцій організації (наприклад, оцінка кредитоспроможності перед отриманням банківського кредиту, оцінка платоспроможності при отриманні комерційного кредиту).

Поточний (або оперативний) фінансовий аналіз проводиться під час виконання конкретного фінансового плану або здійснення конкретної фінансової операції з метою оперативної оцінки результатів фінансової діяльності. Як правило, він обмежується короткими часовими періодами.

Перспективний фінансовий аналіз має на меті показати значення ключових показників, що визначають фінансовий стан і майбутню фінансову стійкість компанії з точки зору їх відповідності цілям розвитку компанії в умовах мінливого зовнішнього і внутрішнього середовища та під впливом прийняття рішень на основі вивчення поточних тенденцій розвитку фінансової ситуації.

Найважливішими завданнями перспективного фінансового аналізу є підготовка аналітичної інформації, необхідної для ілюстрації майбутніх і поточних планів розвитку організації, оцінка реальності виконання планів, а також

Періодичний фінансовий аналіз проводиться регулярно у відповідні періоди (наприклад, річний, квартальний, місячний, щоденний, змінний тощо). Наприклад, річний фінансовий аналіз проводиться для підбиття підсумків фінансової діяльності компанії і слугує основою для розробки або коригування фінансової стратегії організації. Результати річного фінансового аналізу розглядаються вищим керівництвом компанії (радою директорів), а потім представляються на зборах акціонерів.

Регулярний фінансовий аналіз у більш короткі терміни (щомісячний, щоденний) використовується в основному для контролю за досягненням запланованих цілей (ключових показників ефективності) і своєчасного реагування на негативні відхилення.

Разові фінансові аналізи проводяться тоді, коли цього вимагають різні обставини. Наприклад, разовий фінансовий аналіз може бути проведений для виявлення найменш прибуткових або найбільш ризикованих фінансових інвестицій з метою оптимізації інвестиційного портфеля компанії.

Фінансовий аналіз є основою і передумовою для прийняття управлінських рішень щодо формування, накопичення і використання фінансових ресурсів підприємства, вдосконалення їх руху та поточного і довгострокового планування діяльності підприємства.

Фінансовий аналіз включає такі основні напрямки:

1) розподіл грошових потоків відповідно до конкретних планів компанії, визначення обсягу додаткових фінансових ресурсів і каналів їх отримання (кредити, пошук нерозподіленого прибутку, емісія додаткових акцій і облігацій);

2) забезпечення системи фінансової звітності, яка об'єктивно відображає процес і забезпечує контроль за фінансовим станом підприємства;

3) оцінка фінансових потреб підприємства.

Використання фінансового аналізу в управлінні фінансами базується на поясненні його змісту. Зміст фінансового аналізу визначається предметом, цілями і завданнями аналітичної роботи.

Об'єктами фінансового аналізу є фінансово-господарські процеси та операції, фінансові результати діяльності підприємства, економічний потенціал і фінансовий стан підприємства, а також фактори, що визначають результати та ефективність фінансово-господарської діяльності.

Фінансово-господарські процеси (закупівля, виробництво та реалізація продукції (робіт, товарів, послуг)) є об`єктом оцінки динаміки основних параметрів виробництва, реалізації, закупівель в цілому та окремих операцій, вимірювання впливу зовнішніх і внутрішніх факторів, виявлення пріоритетних напрямів розвитку виробництва та резервів.

Для характеристики фінансових результатів діяльності підприємств використовуються такі показники: фінансові результати від операційної діяльності, фінансові результати від звичайної діяльності до та після оподаткування, надзвичайний прибуток (збиток) та чистий прибуток. Аналіз цих показників дозволяє виявити тенденції розвитку підприємства, порівняти отримані результати з фінансовими результатами аналогічних середньогалузевих підприємств та результатами діяльності підприємства за попередній період, виявити причини зміни, оцінити кількісні параметри зміни та в подальшому обґрунтувати прогнозні значення вищезазначених показників.

Економічний потенціал визначається обсягом і складом майна (майновий потенціал) та джерелами фінансування. Фінансовий потенціал - це потенціал підприємства, на основі якого оцінюється фінансовий стан підприємства, що характеризує активи підприємства, залежність підприємства від зовнішніх джерел фінансування, його фінансову стійкість,

платоспроможність і кредитоспроможність. На основі оцінки економічного потенціалу приймаються рішення про капіталовкладення, фінансування та вилучення капіталу.

Фактори, що підлягають фінансовому аналізу - це явища (причини), які впливають на один або декілька показників фінансово-господарської діяльності підприємства і викликають їх зміни протягом досліджуваного періоду.

До них відносяться зовнішні та внутрішні. До зовнішніх факторів належать економічні, політичні, соціальні, кліматичні та екологічні фактори.

Внутрішніми факторами у фінансовому аналізі є фінансові, матеріальні та трудові ресурси. Досліджуючи внутрішні фактори, фінансовий аналіз шукає шляхи позитивного впливу на стан і розвиток внутрішніх факторів відповідно до стратегічних цілей підприємства.

Метою фінансового аналізу є визначення внутрішніх факторів з метою виявлення напрямів підвищення ринкової вартості підприємства та вимірювання резервів на основі вивчення стану і динаміки показників, що характеризують фінансово-господарську діяльність підприємства.

Ця мета досягається шляхом послідовного вирішення завдань фінансового аналізу:

1) аналіз фінансових результатів: оцінка виконання плану за доходами і витратами; аналіз динамічних рядів результативних показників; аналіз формування та розподілу прибутку; аналіз собівартості реалізованої продукції; аналіз факторів формування доходів, собівартості та прибутку; аналіз ефективності використання прибутку;

2) аналіз і прогнозування основних показників, що характеризують фінансовий стан підприємства (фінансової стійкості, платоспроможності та фінансового ризику, оцінка фінансового ризику);

3) аналіз формування та використання фінансових ресурсів;

4) аналіз ефективності використання капіталу;

5) аналіз кредитоспроможності підприємства.

Завдання фінансового аналізу вважається вирішеним, якщо реалізація заходів, розроблених на основі отриманих результатів, забезпечує досягнення поставлених цілей. Досягнення оперативних цілей в кінцевому підсумку призводить до досягнення стратегічних цілей компанії.

Ефективність фінансового аналізу як інструменту управління залежить від дотримання організацією принципів системності, комплексності, об'єктивності, динамічності, точності, оперативності, ефективності та прогресивності.

Принцип системності базується на загальному визначенні управлінської інформаційної системи, яка включає підсистеми аналізу, обліку та контролю.

Принцип системності ґрунтується на побудові фінансового аналізу, що дозволяє вивчити та кількісно оцінити взаємозв'язки між елементами, які складають відповідні рівні економічної системи, що є об'єктом управління.

Принцип комплексності вимагає, щоб усі елементи об'єкта аналізувалися в їх сукупності. Для забезпечення комплексності фінансового аналізу необхідно мати справу з інформацією, що характеризує внутрішні відносини об'єкта дослідження та його взаємовідносини з державою, інвесторами, кредиторами, постачальниками і покупцями.

Принцип об'єктивності стосується насамперед первинної аналітичної інформації, яка має бути повною, репрезентативною (фінансова звітність складається за досить тривалий період часу) та достовірною.

Принцип динамічності вимагає дослідження фінансових ресурсів у динаміці, що дає змогу виявити та оцінити напрями і перспективи розвитку підприємства в цілому та окремих функціональних і структурних підрозділів.

Принцип достовірності ґрунтується на об'єктивній перевірці первинної інформації, точності розрахунків та обґрунтованості зроблених висновків.

Принцип оперативності дає можливість забезпечити оперативний контроль необхідної інформації під час, безпосередньо перед або відразу після здійснення фінансово-господарських операцій.

Принцип оперативності застосовується у двох аспектах:

1) спрямованість аналізу на пошук резервів і методів підвищення ефективності фінансово-господарської діяльності підприємства;

2) витрати на проведення аналізу не повинні перевищувати ефекту від впровадження розроблених заходів.

Принцип прогресивності повинен забезпечити пошук резервів і методів підвищення ефективності використання фінансових, трудових і матеріальних ресурсів підприємства на основі сучасної технології виробництва, високих стандартів управління та організації праці.

Результати аналітичної роботи безпосередньо залежать від якості використовуваної інформації, тому вихідні дані повинні бути ретельно перевірені перед застосуванням. Перед тим, як збирати первинну інформацію, обробляти та систематизувати дані, слід встановити чіткий термін, щоб забезпечити своєчасне надання обробленої інформації для проведення фінансового аналізу на підприємстві. Оскільки реалії сучасного ділового світу характеризуються постійним прискоренням подій, збір, обробка та систематизація інформації для фінансового аналізу повинні здійснюватися, перш за все, швидко.

Систематизацію та підготовку інформаційних джерел для фінансового аналізу можна умовно розділити на два етапи перевірка їх змісту та обробка й аналіз матеріалу.

При проведенні фінансового аналізу на підприємствах повинен здійснюватися процес безперервного цілеспрямованого відбору науково обґрунтованих показників, необхідних для аналізу та підготовки оптимальних управлінських рішень у фінансовій сфері за всіма аспектами фінансового стану, фінансових результатів та інвестиційної привабливості підприємства, тому дані постійно оновлюються, а системи інформаційного забезпечення потребують удосконалення.

На початку проведення фінансового аналізу на підприємстві необхідно здійснити попередню підготовку обраних показників. Підготовка фінансових показників означає, що вихідні показники приводяться до форми, яку можна порівняти між собою, тобто вони є однорідними. Лише у випадку, якщо в процесі фінансового аналізу бажано використовувати багатовимірні методи статистичного аналізу, обов'язковою умовою є приведення фінансових показників до порівнянної форми.

Експерти виокремлюють такі найпоширеніші методи приведення вихідних показників до порівнянної форми:

-нейтралізація вартісних факторів шляхом відображення різних видів кількісних показників в єдиній ціні;

-нейтралізація кількісного фактору шляхом розрахунку набору умовних показників, які не змінюють кількісні показники при аналізі ефективності використання окремих видів ресурсів, але постійно змінюють кількість використаних ресурсів;

-нейтралізація впливу на рівень кількісних та якісних показників методу, що використовується для їх розрахунку;

-розрахунок середніх значень у процесі аналізу великої кількості однотипних показників;

-заміна абсолютних значень на відносні (там, де це доцільно).

Компанії повинні розробити банк методів, моделей і прийомів для використання у фінансовому аналізі. Слід розробити набір сценаріїв найбільш ймовірних подій у зовнішньому та внутрішньому середовищі. Для кожного сценарію слід використовувати чітко визначені інструменти аналізу.

Під час проведення фінансового аналізу повинні бути визначені сильні та слабкі сторони інформації, а також цілісність використання інформації для аналізу та управління економічними і фінансовими процесами та їх наслідками.

Схема взаємозв'язку і взаємозалежності компонентів інформаційно-аналітичного забезпечення для вивчення фінансово-економічних процесів підприємства показана на рисунку 3.

Всі компоненти повинні підбиратися синхронно, комплексно і правильно. У цьому процесі необхідно враховувати всі вимоги до конфіденційності інформації, створення системи індикаторів, набору методів фінансового аналізу та вибору індикаторів.

Ступінь адекватності оцінки та аналізу фінансово-економічних процесів підприємства залежить від правильного визначення фінансового стану підприємства, правильного вибору вимірювача його ознак, тобто системи показників.

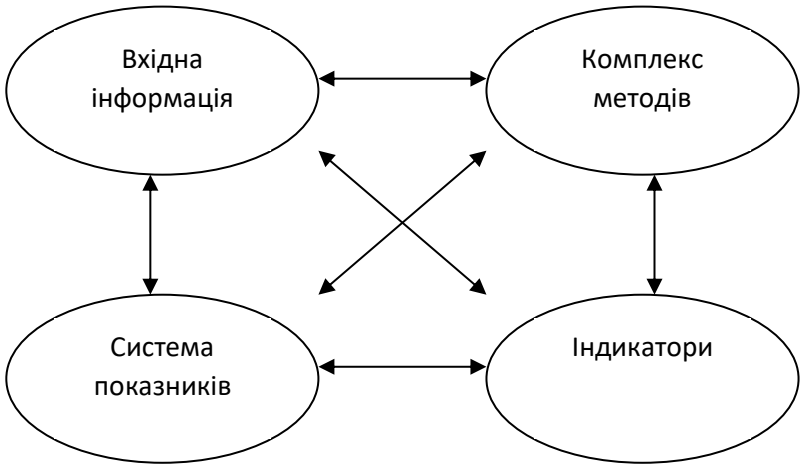


Рис. 3. Схема взаємозв'язку і взаємозалежності компонентів інформаційно-аналітичного забезпечення для вивчення фінансово-економічних процесів підприємства*(Биба В.В., Матюшина Ю.І. 2015)*

Необхідно постійно стежити за фінансово-економічними процесами підприємства, щоб виявити ознаки збільшення або збільшення. У процесі моніторингу фінансово-економічних процесів необхідно враховувати особливості галузі та етапи життєвого циклу, в якому знаходиться підприємство.

Висновки. Таким чином, ефективна система обліково-аналітичного забезпечення прийняття управлінських рішень у ринкових умовах є запорукою стабільного розвитку підприємства та забезпечення його конкурентоспроможності за рахунок своєчасного виявлення та попередження зовнішніх і внутрішніх загроз і небезпек.

В основі обліково-аналітичного забезпечення є інформація, тобто сукупність даних про внутрішнє та зовнішнє середовище підприємства, які використовуються для оцінки та аналізу господарських подій і процесів прийняття управлінських рішень. Основними джерелами для оцінки та аналізу фінансового стану підприємства, фінансових результатів, ефективності використання фінансових ресурсів, кредитоспроможності та інвестиційної привабливості є

фінансова звітність підприємства. Разом з тим, фінансова звітність не може задовольнити всі інформаційні потреби внутрішніх користувачів інформації, а тому з метою надання своєчасної та повної інформації менеджерами для прийняття рішень доцільно сформувати систему управлінського обліку.

Формування на підприємстві ефективної системи обліково-аналітичного забезпечення прийняття управлінських рішень передбачає побудову систем бухгалтерського та управлінського обліку, системи фінансово-економічного аналізу на підприємстві, а також їх взаємозв`язки. З цією метою на підприємстві повинні бути вирішені низка питань. Зокрема, потребує удосконалення система нормативно-правового регулювання облікового забезпечення прийняття управлінських рішень як на державному рівні, так і на рівні облікової політики підприємства.

Важливим завданням підвищення ефективності обліково-аналітичного забезпечення прийняття управлінських рішень є формування управлінського обліку, що передбачає визначення його завдань, об`єктів, предмету, вибір найбільш доцільних методів, розробку та впровадження управлінської оперативної звітності відповідно до інформаційних потреб управлінського персоналу.

Необхідно також сформувати на підприємстві ефективну систему фінансового аналізу, у тому числі, визначити періодичність проведення аналізу, об`єкти, методи тощо.

References:

Про бухгалтерський облік та фінансову звітність в Україні: Закон України від 16 липня 1999 р. № 996-XIV. URL: http://zakon.rada.gov.ua (дата звернення: 31.01.2024)

Міжнародний стандарт бухгалтерського обліку 1 «Подання фінансової звітності» №929 URL: https://zakon.rada.gov.ua/laws/show/929_013#Text (дата звернення: 31.01.2024)

Національне Положення (Стандарт) бухгалтерського обліку 1 «Загальні вимоги до фінансової звітності». Наказ Міністерства Фінансів України від 07 лютого 2013р. №73. URL: https://zakon.rada.gov.ua/laws/show/z0336-13#Text (дата звернення: 31.01.2024)

Господарський кодекс України № 436-IV від 16 січня 2003 р. URL: https://zakon.rada.gov.ua/laws/show/436-15#Text (дата звернення: 31.01.2024)

Податковий кодекс України № 2755-VI від 02 грудня 2010 р. URL: https://zakon.rada.gov.ua/laws/show/2755-17#Text (дата звернення: 31.01.2024)

Національні положення (стандарти) бухгалтерського обліку). URL: https://mof.gov.ua/uk/nacionalni-polozhennja1 (дата звернення: 31.01.2024)

Лист Міністерства фінансів України від 21.12.05 № 31-34000-10-5/27793 «Про облікову політику». URL: http://www.minfin.gov.ua (дата звернення: 31.01.2024)

Лист Міністерства фінансів України «Щодо облікової політики та облікових оцінок» від 14.05.2012р. № 31-08410-07-25/12004. URL: http://www.minfin.gov.ua (дата звернення: 31.01.2024)

Положення (стандарт) бухгалтерського обліку «Виправлення помилок і зміни у фінансових звітах» №173 від 28 травня 1999р. URL: https://zakon.rada.gov.ua/laws/show/z0392-99#Text (дата звернення: 31.01.2024)
Голов С. Ф., Єфіменко В. І. (1996). Фінансовий та управлінський облік. Київ, 1996. 554 с.
Голов С. Ф. (2017). Генезис управлінського обліку. *Бухгалтерський облік і аудит*. 2017. №7-8. С.2-24.
Чумаченко М. Г. (2003). Управлінський облік потребує підтримки. *Бухгалтерський облік і аудит*. 2003. № 5. С. 3-7.
Косташ Т.В., Смола М.Р. (2021). Роль управлінського обліку в прийнятті управлінських рішень. *Ефектива економіка.* № 10. 2021. URL: https://archer.chnu.edu.ua/jspui/bitstream/123456789/2567/1/Kostash%20T.%2C%20Smola%20%D0%9C.%20_article.pdf (дата звернення 31.01.2024).
Косташ Т.В., Карп А.Г. (2021). Роль управлінського обліку в інформаційному забезпеченні управління підприємством. *Міжнародний науковий журнал «Грааль науки»*. № 4. 2021. с. 64-67
Биба В.В., Матюшина Ю.І. (2015). Система управлінського обліку: сутність завдання та етапи впровадження. *Економіка та держава*. №1. 2015. с.60-62.
Задорожний З.-М. В., Аверкин Я. Ф. (2019). Управлінський облік: особливості та принципи. *Фінансово-кредитна діяльність: проблеми теорії та практики*, 2019. №1. С. 114-120.

DOI 10.5281/zenodo.10820490
UDC 351.743.07(477)

CHAPTER 6.
OPTIMIZING PERSONNEL MANAGEMENT IN THE NATIONAL GUARD OF UKRAINE: THEORETICAL FOUNDATIONS, PROBLEMS AND WAYS OF IMPROVEMENT

Andrii HOLOVNIA
Doctor of Philosophy, Senior Lecturer at the Department of Professional Training of the Retraining and Advanced Training Centre of the National Academy of the National Guard of Ukraine
golovnijandr1@ukr.net
https://orcid.org/0000-0001-9188-0055

Volodymyr TROBIUK
Candidate of Military Sciences, Associate Professor,
Head of the Educational and Research Centre for the Organization of the Educational Process of the National Academy of the National Guard of Ukraine,
D1ss@ukr.net
https://orcid.org/0000-0002-3248-2935

Abstract. In modern military management in the context of ensuring national security, the organization of the work of personnel management managers plays a decisive role. The study, devoted to the analysis of existing approaches and methods of personnel management in the National Guard of Ukraine, reveals key problems and shortcomings in the field of organization of activities. The work is focused on the need to improve the scientific basis of labor organization, strengthen the ideological base among military personnel, and develop effective personnel management strategies. In the course of the research, a theoretical analysis of the existing system, analysis of scientific sources, and identification of areas for improvement based on domestic and international experience were carried out. The main results were the development of recommendations for optimizing management processes, increasing the motivation and efficiency of personnel. The study emphasizes the importance of the integration of modern personnel management methods and the implementation of innovative approaches to ensure high combat capability and efficiency of the units of the National Guard of Ukraine. The results of the work are important for the development of theoretical and

practical aspects of military management in Ukraine and can be used for further improvement of the personnel management system in the security and defense sector of the state.

Keywords: personnel management, National Guard of Ukraine, labor organization, management methods, ideological base, management strategies, process optimization, personnel motivation, military management, theoretical analysis.

ОПТИМІЗАЦІЯ ДІЯЛЬНОСТІ УПРАВЛІННЯ ПЕРСОНАЛОМ В НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ: ТЕОРЕТИЧНІ ОСНОВИ, ПРОБЛЕМАТИКА ТА ШЛЯХИ ВДОСКОНАЛЕННЯ

Анотація. У сучасному військовому управлінні в контексті забезпечення національної безпеки, організація праці керівників з управління персоналом відіграє вирішальну роль. Дослідження, присвячене аналізу існуючих підходів та методів управління персоналом в Національній гвардії України, виявляє ключові проблеми та недоліки в сфері організації діяльності. Роботи зосереджена на необхідності удосконалення наукової основи організації праці, зміцненні ідейної бази серед військовослужбовців та розробці ефективних стратегій управління персоналом. В ході дослідження було проведено теоретичний аналіз існуючої системи, аналіз наукових джерел та визначення напрямів вдосконалення на основі вітчизняного та міжнародного досвіду. Основними результатами стали розробка рекомендацій щодо оптимізації управлінських процесів, підвищення мотивації та ефективності персоналу. Дослідження підкреслює значення інтеграції сучасних методів управління персоналом і впровадження інноваційних підходів для забезпечення високої боєздатності та ефективності підрозділів Національної гвардії України. Результати роботи мають значення для розвитку теоретичних та практичних аспектів військового управління в Україні та можуть бути використані для подальшого вдосконалення системи управління персоналом в секторі безпеки і оборони держави.

Ключові слова: управління персоналом, Національна гвардія України, організація праці, методи управління, ідейна база, стратегії управління, оптимізація процесів, мотивація персоналу, військове управління, теоретичний аналіз.

Вступ. В умовах сучасного динамічного розвитку суспільства та зростаючих викликів як до Національної безпеки, так і до державності вцілому, важливість ефективної організації діяльності у сфері військового управління набуває особливої актуальності. Це стосується не тільки стратегічного планування та оперативного управління військовими діями, але й організації дій керівників з управління персоналом, що відіграє ключову роль у формуванні боєздатності та ефективності військових підрозділів в сучасній війні. В цих умовах,

Національна гвардія України (НГУ), яка є однією зі структур, відповідальних за забезпечення внутрішньої та зовнішньої безпеки держави, зіштовхується з необхідністю адаптації своєї системи управління персоналом до сучасних вимог і викликів.

Велике значення в цьому процесі має глибоке розуміння існуючої організації праці, її наукової основи, а також визначення ефективних шляхів її вдосконалення. Це передбачає комплексний підхід, який починається з теоретичного аналізу змісту, завдань та особливостей організації праці керівників, а також глибокого аналізу наукових джерел, що дозволяє виявити і систематизувати існуючі знання та практики в даній сфері.

Одним із ключових етапів є аналіз наукових джерел щодо сутності та змісту формування ідейної бази у військовослужбовців НГУ, що містить вивчення мотиваційних складових, корпоративної культури, лідерства, та їх впливу на ефективність управління персоналом. Це дозволяє не тільки визначити наявні проблеми та недоліки, але й розробити обґрунтовані рекомендації щодо їх вирішення.

Значну увагу в дослідженні приділено визначенню напрямів вдосконалення наукової організації праці, що базується на виокремленні структурних елементів та використанні передового вітчизняного та міжнародного досвіду. Це вміщує аналіз сучасних тенденцій в управлінні персоналом, інноваційних методів та технологій, які можуть бути адаптовані та впроваджені в практику НГУ з метою підвищення її ефективності та боєздатності.

Таким чином, дане дослідження має на меті не лише теоретичний аналіз, але й практичний внесок у вдосконалення організації праці керівників з управління персоналом в органах військового управління та військових частинах, що відповідає актуальним потребам та викликам сучасності. Враховуючи комплексний підхід, викладений у плані дослідження, робота покликана сприяти підвищенню ефективності управлінської діяльності та впровадженню інноваційних підходів у сфері військового менеджменту.

Розділ 1. Теоретичний аналіз змісту, завдань та особливостей існуючої організації діяльності керівників з управління персоналом в НГУ

На основі проведених досліджень теоретичного аналізу змісту, завдань та особливостей організації праці керівників з управління персоналом в органах військового управління та військових частинах НГУ, визначено ознаки, які потребують глибокого вивчення та чіткого усвідомлення для виділення тих догматичних засад, що стануть базовими для службової діяльності керівників з управління персоналом. Першим і головним є розкриття змісту та специфіки роботи керівників з управління персоналом, складовими якого є:

- визначення ролі та обов'язків сучасних керівників з управління персоналом в органах військового управління та військових частинах НГУ;

– означення специфіки військового середовища НГУ.

Розглядаючи роль та обов’язки керівників з управління персоналом, важливо розуміти, що ця робота має багатогранний характер і вимагає комплексного підходу до ряду ключових функцій, що обумовлено унікальністю військового середовища. Забезпечення особливого підходу до кожної ключової функції спирається на Доктрину з планування розвитку в НГУ (*наказ КНГУ, 2023*) де прописані елементи довгострокового, середньострокового та короткострокового планування.

Втілення довгострокового планування відображає розробка та впровадження стратегії управління персоналом. Вона передбачає розробку керівником довгострокових планів, які відображають кінцеві цілі підрозділу, відділу, відділення чи елементу органу управління. Необхідно враховувати і додаткові, проміжні цілі, що загалом є складовими довгострокового планування і забезпечують його безперервність та поточний контроль. Задоволення військових вимог та потреб в даній системі є домінуючим фактором, врахування якого унеможливить відхилення від визначеного напрямку діяльності. Велике значення в стратегічному плануванні відіграють гнучкість та адаптивність. Як показують сучасні кризові умови діяльності, стратегії мають бути гнучкими, щоб адаптуватися до швидко змінюваних військових умов, що залучать соціальну, технологічну, економічну складові тощо. Врахування зовнішніх факторів впливу на неї дозволять мінімізувати негативний вплив та активувати продуктивну взаємодію з галузями, структурами, організаціями, фондами та спілками, що ставлять за мету розвиток оборонного потенціалу як держави вцілому, так і НГУ зокрема.

Втілення середньострокового планування відображається в плануванні кадрової політики з чітким баченням проміжної мети та цілі конкретного етапу підрозділу, відділу чи відділення. Ключову роль тут відіграє ідентифікація критичних позицій, втілених у нормативно-правових рамках діяльності кожного підрозділу. Адже врахування специфіки службово-бойових завдань (СБЗ), що виконує НГУ веде за собою особливі умови виконання і як наслідок, затверджує перелік вимог до кожної особистості на конкретній військовій посаді. Завданням керівників з управління персоналом є врахування цих позицій, і чим вищій щабель у військовій ієрархії займає керівник, тим більше таких специфічних вимог йому необхідно враховувати. Для автоматизації та стандартизації даних процесів є дієвим процес визначення та формалізації компетенцій посад (в симбіозі професійного розвитку та дії системи мотивації до професійного розвитку) кожного підрозділу. Наслідки такої діяльності закономірно втілюються у розробку кар'єрних шляхів. Це створення чітких алгоритмів, траєкторій та методів кар'єрного росту, важливих для мотивації та утримання персоналу. Максимальна візуалізація цих моделей та процесів надасть такі переваги, як чіткість та прозорість кар'єрних

шляхів, стале планування розвитку особистості, краще розуміння організаційної структури, забезпечення об'єктивності та справедливості в діяльності військового формування, підтримка управлінських рішень, залучення та утримання найкращих фахівців.

Короткострокове планування реалізовано в процесах кадрового відбору, диверсифікації кадрів, адаптації, навчанні, оцінюванні та розвитку військового персоналу. Обов'язковим є уточнення, що вище зазначені процеси можуть виступати складовими довго та середньо строкового планування але в інших елементах системи військового формування та її діяльності. Нас цікавить кінцевий результат організації праці керівників з управління персоналом, реалізація дії «в полі», «на землі», при безпосередньому контакті з особистістю.

Тож процес організації праці керівників з управління персоналом реалізує розробку ефективних механізмів відбору кандидатів, які відповідають вимогам військової служби. Диверсифікація кадрів сприяє залученню різноманітних груп населення, що є важливим елементом сучасного управління персоналом, в обставинах створення службового середовища, де представлені військовослужбовці різного віку, статі, етнічного походження, релігійних переконань, сексуальної орієнтації та інших характеристик. Це сприяє поліпшенню інноваційності та креативності, як наслідок підвищується ефективність роботи та її результати. Також задовольняється складова соціальної справедливості та рівності можливостей для різних груп населення. Підвищується задоволеність та мотивація персоналу, що поліпшує репутацію організації у суспільстві.

Другою складовою розкриття змісту та специфіки роботи керівників з управління персоналом є означення специфіки військового середовища НГУ. Воно є основним напрямом управління персоналом вцілому, так як НГУ має стратегічне значення в системі Національної безпеки та оборони країни. Дана тема вимагає детального розгляду трьох ключових елементів: військової ієрархії, військової дисципліни та адаптації до унікальних військових умов та вимог.

Ієрархічна структура військового середовища є фундаментальною особливістю військових формувань з набором специфічних характеристик. Чітке розмежування відповідальності у військовій ієрархії характеризується індивідуально визначеними ролями, де кожна посадова особа виконує певні обов'язки та відповідає за них. Дотримання субординації та принципу прямого та безпосереднього підпорядкування, прописаних у Дисциплінарному статуті Збройних Сил України (*Закон України, 1999*), передбачає дотримання кожним елементом системи від найвищого до найнижчого рангу визначеного принципу єдино начальництва. У вказаній діяльності командування несе відповідальність за прийняття оперативних рішень, тоді як нижчі ранги виконують завдання та відповідають

відповідно на тактичному рівні. Це непохитний та основоположний принцип діяльності військової структури, який необхідно дотримуватись при організації управління персоналом в органах військового управління військових частин НГУ.

Військова дисципліна є складовою військового середовища в організації праці керівників з управління персоналом, вона полягає у сумлінному дотриманні визначених правил та процедур, які є критичними як при виконанні СБЗ, так і при повсякденній службово-бойовій діяльності (СБД). Для підтримання високого рівня дисципліни керівники з управління персоналом повинні зважено використовувати системи заохочень та покарань, не забуваючи бути прикладом для підлеглих. Також керівники повинні забезпечувати адаптацію до унікальних військових реалій, так як військове середовище часто характеризується швидкими змінами, які вимагають від персоналу здатності швидко пристосовуватися. Виконання даної умови забезпечить постійне навчання та розвиток набутих навичок. Не слід нехтувати також психологічною підтримкою, адже врахування психологічної грані адаптації надважливе у діяльності підлеглого військовослужбовця як у пункті постійної дислокації, так і при виконанні бойових завдань у відрядженні.

Кожна з цих складових вимагає детального вивчення та інтегрованого підходу в рамках управління персоналом. Врахування специфіки військового середовища є критичним у сфері ефективного управління та розвитку персоналу в таких умовах.

Другою характеристикою особливостей організації праці керівників з управління персоналом в органах військового управління та військових частинах НГУ, які потребують глибокого вивчення для забезпечення якісної діяльності керівників з управління персоналом є активація та впровадження процесу діяльності керівників з управління персоналом, складовими якого є:

- оптимізація діяльності та підвищення ефективності виконання СБЗ, СБД;
- мотивація та утримання кваліфікованого персоналу у військовій сфері.

Оптимізація військової діяльності та підвищення ефективності виконання СБЗ, СБД стоять в центрі сучасних військових стратегій. Це складне завдання, яке охоплює ряд викликів та цілей, пов'язаних як з управлінням ресурсами, так і з тактикою та стратегією ведення бойових дій.

Одним із ключових викликів є адаптація до швидко змінюваних технологічних умов та зовнішнього середовища. Розвиток технологій, особливо в сферах протиповітряної оборони, кібербезпеки та автоматизованого військового обладнання, вимагає неперервного оновлення військових стратегій та методик навчання. Це також стосується розуміння та застосування нових форм ведення військових дій, які можуть включати гібридні та асиметричні конфлікти.

Важливою складовою оптимізації військової діяльності є управління людськими ресурсами, забезпечення високої моральності та психологічної стійкості персоналу, враховуючи високі ризики та стресові ситуації. Потрібен ефективний підбір та підготовка персоналу, щоб гарантувати наявність необхідних навичок та здібностей для виконання СБЗ. Окрім цього, значущим є питання мотивації та утримання кваліфікованих спеціалістів, здатних оперативно реагувати на сучасні виклики військової агресії та протиправної діяльності.

Оптимізація логістичних та операційних процесів також відіграє ключову роль, так як ефективне управління ресурсами, об'єднуючи озброєння, амуніцію, обладнання та бойову підтримку, є необхідним для успішного виконання бойових завдань. Це містить розробку та впровадження систем управління, які можуть адаптуватися до змінних умов та потреб. Питання інформаційної безпеки та кіберзахисту стають все більш актуальними. Захист інформаційних систем від зовнішніх загроз, а також забезпечення надійного обміну інформацією є важливими елементами сучасних військових стратегій.

Оптимізація військової діяльності у сфері протиповітряної оборони супроводжується низкою специфічних викликів та цілей, які визначають ефективність системи захисту від повітряних загроз. Враховуючи динамічний характер сучасного протистояння у повітряному просторі та швидкий розвиток технологій, ці виклики та цілі потребують особливої уваги. Одним з основних викликів є інтеграція новітніх технологій у системи протиповітряної оборони. Вона забезпечує розвиток та впровадження сучасних радіолокаційних систем, засобів знищення повітряних цілей, а також систем управління та комунікації. Сучасна протиповітряна оборона повинна ефективно протистояти різноманітним загрозам, таким як безпілотні літальні апарати, крилаті ракети, та традиційну авіацію. Адаптація до змінюваних умов бойових дій на фоні політичного контексту є ще одним критичним елементом, адже протиповітряна оборона повинна бути гнучкою та здатною швидко реагувати на зміни у характері загрози. Це потребує постійного аналізу розвідувальних даних, вивчення потенційних загроз та розробки сценаріїв для їх нейтралізації.

Особливу увагу потрібно приділяти підготовці та навчанню персоналу. Військовослужбовці, задіяні у протиповітряній обороні, повинні мати високий рівень професійної підготовки та бути здатними ефективно використовувати складне обладнання. Це вимагає постійного оновлення навчальних програм, враховуючи останні технологічні та тактичні розробки на основі досвіду бойових дій перш за все. Особливим є також забезпечення координації дій між різними підрозділами протиповітряної оборони, а також іншими видами військ, адже ефективна комунікація та співпраця є ключовими для створення єдиної та

ефективної оборонної системи. Необхідно також враховувати питання економічної ефективності, оптимізація військової діяльності в сфері протиповітряної оборони вимагає значних фінансових інвестицій, тому необхідно забезпечувати раціональне використання ресурсів, оцінювати ефективність інвестицій та шукати шляхи зниження витрат без втрати бойової готовності.

Врахування вказаних положень дозволить керівникам з управління персоналом підвищити ефективність та адаптивність своєї діяльності. Ефективне управління ресурсами, постійне оновлення та адаптація стратегій, а також зосередження на розвитку та підтримці військового персоналу є ключовими для досягнення успіху в сучасних надскладних умовах війни.

Систематичне навчання та професійний розвиток є фундаментальними елементами у забезпеченні військової ефективності, постійне оновлення знань та навичок військовослужбовців є ключовим для підтримання боєздатності та готовності до виконання СБЗ та СБД підрозділів НГУ. У військових рамках діяльності НГУ, де вимоги до точності, дисципліни та ефективності є високими, постійне оновлення та вдосконалення професійних знань є критично важливим. Через систематичне навчання військовослужбовці не тільки підтримують свої базові навички на належному рівні, але й набувають нових компетенцій, необхідних для роботи з сучасним обладнанням та в нових бойових умовах.

Крім того, систематичне навчання допомагає підтримувати високий рівень готовності до різних викликів, з якими може зіткнутися військовий персонал. Це особливо актуально в теперішній час, коли характер бойових дій постійно змінюється і загрози стають все більш різноманітними та складними. У військовій ієрархії, де правильне прийняття рішень та здатність керувати іншими мають вирішальне значення, навчання лідерства та управлінських навичок є ключовим, воно містить не тільки традиційні особливості військового лідерства, але й сучасні підходи командної взаємодії, мотивації та ефективної комунікації. Систематичне навчання також сприяє підвищенню морального духу та задоволеності військового персоналу. Військовослужбовці, які регулярно проходять курси підготовки та розвивають свій потенціал, відчувають більше задоволення від своєї роботи.

Таким чином, систематичне навчання та розвиток військових кадрів є невід'ємною частиною оптимізації військової діяльності, забезпечуючи адаптивність, готовність та ефективність НГУ.

У сфері військової професійної підготовки НГУ система навчання охоплює широкий спектр програм, які варіюються від базового військового до спеціалізованих курсів, що відповідають конкретним потребам військовослужбовців. Ці навчальні програми мають на

меті не лише забезпечити необхідні навички та знання для ефективного виконання СБЗ, але й розвивати особистісні якості та компетенції, необхідні для успішної військової кар'єри.

Базове військове навчання є основою для кожного військовослужбовця. Цей етап навчання зосереджений на виробленні базових військових знань, умінь та навичок. Він включає фізичну підготовку, навчання основам тактики, знайомство з військовою дисципліною та військовою ієрархією. Базове навчання також забезпечує основні знання з використання зброї, діяльність та виживання у бойових умовах та невідкладної медичної допомоги. Цей етап навчання відіграє важливу роль у формуванні військової етики та вихованні почуття відповідальності.

На наступному етапі, військовослужбовці можуть пройти навчання, яке забезпечує більш глибоке розуміння військових спеціалізацій та функцій. Такі програми охоплюють спеціалізовані тактичні, фахові курси, курси лідерства, а також технічні та технологічні тренінги. На цьому етапі військовослужбовці набувають більш глибоких знань у конкретній області, таке навчання не тільки розширює професійні горизонти, але й допомагає розвивати критичне мислення та прийняття рішень у складних ситуаціях. Для військовослужбовців, які прагнуть досягти вищих посад доступні програми навчання військових лідерів. Ці курси зосереджені на розвитку управлінських навичок, стратегічного планування, а також на вивченні принципів військового командування та контролю, навчання містить аналіз військових операцій, управління ресурсами, а також етичні та моральні аспекти військового лідерства.

Тож різні рівні навчальних програм відіграють критичну роль у підготовці та розвитку військових кадрів. Від базового навчання до спеціалізованих курсів та програм лідерства, систематичне навчання забезпечує необхідну підготовку, яка дозволяє військовослужбовцям ефективно виконувати свої завдання та професійно розвиватися.

Кваліфіковані викладачі, інструктори та навчальний персонал відіграють ключову роль у процесі військової підготовки, що є вирішальним фактором для ефективності та готовності військовослужбовців до СБД. Їхня робота не просто полягає в передачі знань і навичок, але й у формуванні військових цінностей, професійної етики та бойового духу серед курсантів та молодших офіцерів.

Викладачі та інструктори забезпечують актуальність, комплексність та відповідність сучасним військовим/освітнім стандартам та вимогам військового навчання та підготовки. Вони повинні постійно оновлювати свої знання та навички, щоб відповідати швидко змінюваним технологіям та тактичним підходам у військовій сфері. Тобто, викладачі повинні не лише глибоко розуміти теоретичні грані військової науки, але й постійно слідкувати за

новітніми розробками та інноваціями. Крім професійних та технічних знань, вони відіграють ключову роль у розвитку лідерських якостей та вмінні приймати рішення. Вони формують у військовослужбовців вміння критично мислити, аналізувати складні ситуації та ефективно реагувати в умовах стресу та невизначеності. Ці навички є вирішальними для успішного виконання СБЗ в реальних бойових умовах.

Важливим виміром роботи навчального персоналу є вміння мотивувати та надихати слухачів. Вони повинні вміти створювати позитивне та заохочуюче навчальне середовище, де особистість може розвиватися як фізично, так і інтелектуально. Від цього часто залежить, наскільки ефективно військовослужбовці зможуть застосувати отримані знання та навички у майбутньому. Особливо суттєвою є роль інструкторів у періоди бойових дій або кризових ситуацій, коли вимоги до військових сил швидко зростають, а потреба в якісному навчанні та підготовці стає критичною. В цих умовах інструктори відіграють роль ключових фігур, що забезпечують швидку та ефективну адаптацію військових кадрів до нових викликів та умов.

Підсумовуючи зазначимо, що кваліфікований навчальний персонал, що надає різні рівні навчальних програм та забезпечує систематичне навчання та підготовку є фундаментом успішного виконання СБЗ та СБД. А ефективне управління ресурсами, постійне оновлення та адаптація стратегій в поєднанні з вище вказаним, дозволить керівникам з управління персоналом підвищити ефективність та адаптивність своєї діяльності.

Досліджуючи визначення важливості мотивації та утримання кваліфікованих кадрів у військовій сфері, необхідно зосередитися на ролі, яку відіграє мотивація у роботі з військовим персоналом. Сучасна військова парадигма характеризується швидкими технологічними змінами, зростаючою складністю бойових дій та постійно змінюваними геополітичними реаліями. У таких умовах мотивація та утримання кваліфікованого військового персоналу набуває особливої актуальності. Ключовим в сучасній війні є не лише технологічна перевага, а й готовність та здатність військовослужбовців ефективно використовувати ці технології, адаптуватися до нових умов та виконувати завдання під впливом високого рівня стресу.

Мотивація військового персоналу залежить від ряду факторів, що містять кар'єрні можливості, відчуття власної значущості та участі у продуктивній діяльності підрозділу, а також від особистісного та професійного розвитку. Ефективне управління мотивацією та утриманням персоналу також є необхідним для підтримання високого рівня бойового духу, моральної та психологічної готовності. Це, у свою чергу, безпосередньо впливає на загальну ефективність військових підрозділів НГУ та визначає результат СБЗ.

Система мотивації військового персоналу, що є складовою комплексної стратегії управління персоналом, відіграє принципову роль у досягненні ряду ключових цілей. Вони є

зорієнтованими як на забезпечення поточних потреб підрозділів, так і на створення основи для довгострокової ефективної діяльності НГУ.

Перш за все, ефективна система мотивації прагне підвищити загальне задоволення військовослужбовців їхньою службою. Задоволений персонал є більш мотивованим та відданим своїй справі, що позитивно впливає на загальну атмосферу та психологічний стан у військових частинах, підрозділах тощо. Підвищення задоволеності військовою службою може бути досягнуто через різні ініціативи, включаючи визнання досягнень, надання можливостей для професійного росту, забезпечення адекватних умов СБД з врахуванням особистих потреб та інтересів персоналу.

Другою важливою метою є зниження рівня відтоку кваліфікованого персоналу. Втрата досвідчених та кваліфікованих військових кадрів може негативно впливати на ефективність СБЗ та потребує значних зусиль та ресурсів для підготовки нових спеціалістів. Система мотивації, яка враховує потреби та бажання персоналу, може допомогти утримати фахівців, пропонуючи їм перспективи кар'єрного росту, конкурентні умови СБД та відчуття власної значущості у виконуваних СБЗ. Система мотивації спрямована на підвищення загальної ефективності військових кадрів. Мотивований персонал, який відчуває підтримку та цінується, має більшу ймовірність ефективно виконувати свої завдання, проявляти ініціативу та вносити вклад у досягнення загальних цілей військового формування, відповідно це призводить до підвищення якості виконання завдань, краща адаптацію до змінних обставин та ефективніша реалізація стратегічних ініціатив. Система мотивації залучає не тільки матеріальні стимули, але й психологічну підтримку, розвиток кар'єрних можливостей, створення позитивного робочого середовища та визнання внеску кожного військовослужбовця.

Аналіз потреб персоналу є необхідним для розробки ефективної системи мотивації для організації діяльності керівників з управління персоналом у військовій сфері, він розкриває глибоке розуміння як професійних завдань та обов'язків військовослужбовців, так і їхніх особистих очікувань, цінностей та амбіцій. Військова служба містить високий рівень стресу, ризик для життя та здоров'я, а також необхідність дотримання строгих військових норм та дисципліни і потреби військовослужбовців закономірно включають як питання кар'єрного росту та матеріальної компенсації, так і забезпечення безпеки, стабільності та підтримки на особистому рівні.

Ефективний аналіз потреб персоналу містить детальне дослідження різних сторін їхнього професійного та особистого життя. Це може бути реалізовано через опитування, анкетування, інтерв'ю, фокус-групи та аналіз робочої поведінки. Такий підхід дозволяє зібрати

цінну інформацію про очікування, переваги та проблеми, з якими стикаються військовослужбовці у своїй повсякденній діяльності. На основі зібраної інформації можна розробити цілеспрямовані програми мотивації, які враховують реальні потреби військового персоналу. Такі програми передбачають різноманітні ініціативи, від систем винагород і визнання до можливостей професійного розвитку, покращення умов СБД, забезпечення психологічної підтримки та створення сприятливого службового середовища. Особливу увагу слід приділити питанням здоров'я та безпеки, а також забезпеченню прийнятного балансу між військовою службою та особистим життям. Значущим є також постійне супроводження ефективності системи мотивації та адаптація її до змінюваних умов та потреб військового персоналу. Врахування зворотного зв'язку від військовослужбовців та гнучкість у зміні підходів дозволить системі мотивації бути ефективною та відповідати реальним умовам сьогодення.

Тож аналіз потреб персоналу та розробка на його основі ефективної системи мотивації служить для забезпечення задоволеності, ефективності та відданості військових кадрів і сприяє підвищенню оперативної готовності, ефективності підрозділів та формує основу довгострокової діяльності НГУ.

Роль нагород та заохочень у військовій сфері є дієвим рушієм у створенні мотивуючого середовища, що сприяє високому моральному духу та підтримує аспірації персоналу до досягнення вищих стандартів професіоналізму. У сфері, де ризики високі та вимоги до військовослужбовців часто межують із крайнім фізичним та психологічним навантаженням, визнання за сумлінну службу відіграють ключову роль у підтримці мотивації та відданості.

Система визнання досягнень вирішує ряд фундаментальних питань.

По-перше, вона діє як засіб підтримки професійних цінностей та стандартів, виховуючи почуття гордості за приналежність до військової організації. Нагородження за видатну службу та інші досягнення не тільки визнають індивідуальний вклад військовослужбовців, але й служать як приклад для інших, стимулюючи їх до подальшого розвитку та вдосконалення.

По-друге, система визнання та нагород сприяє створенню позитивної атмосфери конкуренції та спонукання до самовдосконалення. Відзнаки та нагороди часто вважаються знаком високого професіоналізму та ефективності, що мотивує військовослужбовців досягати високих результатів у своїй службі. Це створює здорове середовище, де кожен прагне до професійного вдосконалення та демонструє високу відданість при виконанні обов'язків.

Третьою складовою є вплив системи визнання на формування позитивних традицій у підрозділах. Нагороди та відзнаки підкреслюють значення ключових цінностей, таких як

честь, відданість, відвага, та відповідальність, це сприяє зміцненню ідентичності та культурних норм НГУ.

Однак, необхідно, щоб система визнання та нагород була справедливою та прозорою. Необхідно забезпечити, щоб усі досягнення оцінювалися об'єктивно, а процес нагородження був зрозумілий та доступний для всіх членів військової організації. Це гарантує, що відзнаки та нагороди сприймаються як дійсно заслужені та значимі. Визнання та нагороди відіграють вирішальну роль у створенні позитивної динаміки як в межах військової структури так і поза нею, сприяючи оптимізації поточної діяльності та підготовці до майбутніх викликів. Через ці інструменти можна ефективно культивувати високий рівень професіоналізму та готовності до виконання СБЗ.

Розділ 2. Аналіз наукових джерел щодо сутності та змістовності формування ідейної бази у військовослужбовців НГУ

Значення ідейної бази для військовослужбовців є одним із фундаментальних аспектів військової культури. Ідейна база, яка охоплює цінності, переконання, традиції та норми, що формує етичний кодекс НГУ, має вирішальну роль у формуванні професійної ідентичності та поведінки військовослужбовців. Вона визначає моделі, у яких військовослужбовці сприймають свою роль у суспільстві, відповідальність перед державою та громадянами, а також впливає на готовність до виконання СБЗ.

Ідейна база, з огляду на сучасне військове управління, стає особливо важливою при ускладненні бойових завдань та змін у глобальному безпековому середовищі. Її розробка та еволюція висвітлена в роботах Єрьоменка Е. (*Єрьоменко Е., 2014)*, Муляви В., Богайчука В. (*Мулява В., Богайчук В., 2020)*. Вона сприяє розвитку згуртованості військових колективів, зміцненню морального духу, а також забезпечує етичну орієнтацію в складних ситуаціях, які можуть включати моральні та етичні дилеми.

Формування міцної ідейної бази вміщує систематичне навчання, культурне виховання, а також постійне підкріплення через військові традиції та ритуали. Це також забезпечує створення середовища, в якому підтримуються та розширюються ключові цінності, такі як честь, відданість, відповідальність та патріотизм.

Однак розвиток ідейної бази також піддається впливу змін, що відбуваються у суспільстві країни та світовій спільноті. Війна внесла свої корективи, як розкрито в роботі Пашкова О.О. (*Пашкова О.О., 2019)*, і сучасні військові структури, як НГУ зокрема, зіштовхуються з потребою адаптації своїх ціннісних систем до глобальних гуманітарних стандартів, змін у міжнародному праві та зростаючої обізнаності соціальних та культурних вимог. Ідейна основа для військовослужбовців залишається не тільки у формуванні

індивідуальної свідомості та професійної поведінки, але і в утворенні фундаменту ефективної військової діяльності організації, яка здатна адаптуватися до викликів сучасного світу, зберігаючи при цьому свої основні цінності та принципи.

Формування ідейної бази у військовій сфері є багатовимірним процесом, який спирається на ряд ключових концепцій, зокрема ідентичність, цінність та мотивацію. Ці поняття складають основу для розуміння того, як військовослужбовці сприймають себе, своє місце в підрозділі та роль у суспільстві загалом. Концепція ідентичності відіграє основну роль у формуванні ідейної бази, що охоплює внутрішнє усвідомлення військовослужбовцями своєї ролі, статусу та належності до військового колективу. Ідентичність особистості військовослужбовця формується через соціалізацію, навчання, взаємодію з колективом та участь у спільній СБД, вона містить професійну гордість, відданість військовим цінностям та почуття власної значущості у виконанні важливої суспільної справи.

Мотивація є тією складовою концепції, яка впливає на формування ідейної бази, вона спонукає військовослужбовців до дій, розкриває бажання досягти успіху та визнання. Ефективна мотивація розкриває як внутрішні мотиватори, такі як особисте задоволення від виконання обов'язків, так і зовнішні, як наприклад, система винагород та кар'єрні можливості.

Таким чином, розуміння та впровадження складових концепції – ідентичності, цінностей та мотивації – є результатом розвитку міцної та ефективної ідейної бази НГУ.

Сучасні медіа та технології мають значний вплив на формування ідейних установ військовослужбовців, що є досить значущим в умовах сучасного інформаційного суспільства. Широке розповсюдження інформаційних технологій та засобів масової комунікації спричиняє зміни в тому, як військовослужбовці сприймають навколишній світ, формують власні переконання та цінності, а також взаємодіють один з одним та з суспільством. Загальні тенденції цих напрямків розкрили науковці Макух-Федоркова І. (*Макух-Федоркова І., 2021),* Набока С. (*Набока С., 2022)*.

Вплив сучасних медіа на військових зосереджується переважно на двох рівнях: з одного боку це зовнішнє інформаційне середовище, яке формується за допомогою новин, соціальних мереж та інших комунікаційних платформ, з іншого – внутрішні комунікаційні системи, які використовують для координації дій та обміну повідомленнями в середині військового формування, НГУ зокрема.

Зовнішнє медіа-середовище часто впливає на формування суспільних уявлень про військову службу, бойові дії тощо. Військовослужбовці, як активні учасники суспільства, не залишаються осторонь від цього впливу, адже інформація, отримана з медіа, може вплинути на їхні ідейні установки та переконання.

Внутрішні комунікаційні системи та технології мають ключову роль у формуванні ідейних установ військовослужбовців. Це забезпечує використання спеціалізованих платформ для навчання та розвитку, системи управління інформацією, які можуть ефективно координувати дії та розподіляти ресурси, а також платформи для внутрішнього спілкування та обміну думками. Такі технології дозволяють не тільки підтримувати ефективну робочу взаємодію, але й сприяють розвитку спільних цінностей та норм, які є основою для згуртованості та ефективної роботи військового колективу.

Таким чином, для сучасного військового управління роль медіа та технологій не може бути недооцінена, вони мають вирішальну роль у тому, як військовослужбовці сприймають себе та свою роль у суспільстві, формують своє переконання та цінності, а також як вони спілкуються та взаємодіють один з одним. Врахування цього впливу допомагає розробкам ефективних стратегій управління та розвитку військових кадрів.

У сучасному інформаційному просторі, де інформаційні війни, пропаганда та фейкові новини стали загальнопоширеними, наукова спільнота все більше зосереджує увагу на вивченні їх впливу на формування ідейних установ військового середовища. Це питання є особливо актуальним, так як інформаційні операції мають великий потенціал впливу на переконання, цінність та моральні орієнтири військовослужбовців, а також на загальне сприйняття військової системи громадськістю. В сучасних наукових дослідженнях це питання вивчали Драбюк С. (*Драбюк С., 2022)*, Шульська Н. М., та Зінчук Р. С. (*Шульська Н. М., Зінчук Р. С., 2022)*.

Інформаційні війни, які залучають стратегічне використання інформації для військових цілей, ставлять за мету дезорієнтуючий вплив на військових, викликаючи надійність отриманої інформації. Пропаганда, яка часто використовується для маніпулювання громадською думкою та формування певного образу бойових дій, забезпечення, управління, може впливати на моральний дух військовослужбовців та їх сприйняття власної ролі у виконанні СБЗ та СБД.

Феномен фейкових новин, або поширення недостовірної інформації, став особливо актуальним в сучасних умовах широкого доступу до інтернету та соціальних мереж. Розповсюдження неправдивої інформації може призвести до неправильного розуміння ситуацій, викликати плутанину та недовіру, а також може бути використане як засіб психологічного тиску на військовослужбовців. Наукові дослідження цієї галузі зосереджуються на аналізі механізмів впливу цих феноменів на ідейну базу військових формувань. Важливим є вивчення того, як інформаційні війни та пропаганда впливають на формування переконань та цінностей військовослужбовців, а також розуміння ефективних

стратегій розвінчання фейкових новин та підтримки об'єктивного та критичного сприйняття інформації. Особливо цінними є дослідження дієздатності ефективного протистояти спотворенню інформації та збереження стабільності та ефективності у мінімальному інформаційному середовищі.

З огляду на це роль сучасних медіа та технологій у формуванні ідейної бази військовослужбовців вимагає комплексного підходу до аналізу та розуміння, який включає вивчення впливу інформаційних воєн, пропаганди та фейкових новин. Такий підхід є ключовим для забезпечення стійкості військових кадрів та підтримки їх здатності до критичного мислення та ефективного реагування на виклики сучасного інформаційного світу.

В середовищі вивчення впливу лідерських якостей та культури на формування ідейних установ у військовому колективі, науковий інтерес зосереджується на розумінні того, як лідерство з культурною складовою впливають на цінності, переконання та норми, які домінують у військовому середовищі. Зокрема це досліджено в роботах Усаченка О. О. (*Усаченко О. О., 2022)*, Заруби О. (*Заруба О., 2019)*, Алещенка В. (*Алещенко В., 2022)*.

Лідерські якості змінюють комунікаційні навички та здатність впливати на інших, формують ідейні установки у військовому колективі. Ефективні лідери можуть впроваджувати та зміцнювати певні цінності та норми, стимулюючи військовослужбовців до їх прийняття та підтримання. Лідери впливають також на формування ідентичності та сприйняття ролі військовослужбовців у суспільстві.

Культурна складова у військових колективах охоплює загальні цінності, переконання, звичаї та традиції, які формуються з часом та відображають історію та бойовий шлях військового формування. Вона впливає на поведінку та сприйняття військовослужбовців, визначаючи, як вони взаємодіють собою між собою, реагують на зовнішні події та виконують свої службові обов’язки. Створення та підтримка позитивної та здорової культури організації сприяє підвищенню згуртованості та морального духу НГУ.

Потребує вивчення те, як різні складові лідерства та культури організації взаємодіють та впливають один на одного, формуючи унікальне середовище, в якому військовослужбовці розвиваються та функціонують. Аналіз цих зв’язків може допомогти у визначенні факторів сприяння успішного формування ідейних установ, підвищуючи ефективність виконання СБЗ і забезпечуючи адаптивність до глобальних змін.

Формування ідейної бази військовослужбовців, яке охоплює їх цінність, переконання та етичні норми, несе в собі низку етичних та моральних викликів. У сучасному світі, де бойові дії та їх дослідження є предметом широкого громадського інтересу, питання моралі та етики набувають особливої актуальності.

Ключовим фактором етичних викликів є визначення межі між військовою потребою та загальнолюдськими цінностями. Це активує питання дотримання правил ведення війни, захисту цивільного населення, а також етичного ставлення до противника. Дана проблематика розглянута вченими Севрук, І. та Соколовською Ю. (*Севрук, І., Соколовська Ю., 2022)*.

Військовослужбовці повинні бути здатні прийняти рішення, яке відповідає не тільки тактичним чи оперативним завданням, але й загальнолюдським етичним нормам. Не менш важливим є вплив ідейних установ на поведінку військовослужбовців за межами бойових дій: взаємодію з цивільним населенням, поведінку в соціумі та виконання повсякденних обов'язків. Формування морально-етичних стандартів дозволяє підтримати позитивний імідж військових НГУ з боку громадян.

Проблема виховання та підтримки етичних стандартів серед військовослужбовців містить розробку та впровадження програми етичного навчання, підвищення обізнаності про дослідження етично сумнівних рішень та дій, а також розвиток системи відповідальності та саморегуляції.

Розділ 3. Наукове обґрунтування напрямів вдосконалення організації діяльності керівників з управління персоналом НГУ.

В сучасному умовах зростаючих глобальних викликів та складності військових операцій, важливість науково обґрунтованої організації праці керівників з управління персоналом набуває особливої актуальності. Це насамперед стосується органів військового управління підрозділів НГУ. Ефективне управління персоналом є ключовим для забезпечення високої боєздатності, оперативної готовності та адаптивності військових підрозділів до змінюваних умов та викликів. Центральною складовою є визначення напрямів вдосконалення наукової організації праці керівників з управління персоналом. Це передбачає аналіз та оцінку існуючих підходів та методів, виявлення потенційних слабких місць та розробку стратегій оптимізації управлінської діяльності на основі виокремлення структурних елементів наукової організації праці. Виокремлення структурних елементів наукової організації праці дозволило забезпечити особливий підхід до кожної ключової функції, що спирається на Доктрину з планування розвитку в НГУ(*наказ КНГУ, 2023*), тож всі наукові дослідження повинні спиратися на елементи довгострокового, середньострокового та короткострокового планування.

Такий підхід містить системний аналіз різних складових управлінської діяльності, охоплюючи планування, організацію, мотивацію та контроль. Принциповим є також вивчення міжнародного досвіду та адаптація найкращих світових практик до умов та специфіки Національної гвардії України. Це дозволяє не лише покращити ефективність військового

управління, але й забезпечити відповідність сучасним вимогам та стандартам. Урахування специфіки військового управління, особливостей військової культури та традицій, а також змін на сучасному геополітичному та технологічному фоні є вирішальними для розробки ефективних стратегій наукової організації праці.

Таким чином, цей науковий аналіз спрямований на вдосконалення управління персоналом у військових органах з урахуванням вітчизняного досвіду та глобальних тенденцій.

Тож розробка кадрової політики НГУ є, на нашу думку, пресупозицією в напрямках вдосконалення організації діяльності керівників з управління персоналом в органах військового управління підрозділів НГУ. Вона ґрунтується на принципах вивіреності, збалансованості та ставить за мету забезпечення виконання стратегічних, оперативних, тактичних цілей військового формування та максимальне задоволення потреб ключового елементу системи – військовослужбовця.

А першочерговим завданням керівників є найбільш продуктивне виконання цих вимог за вказаними принципами. В основі кадрової політики повинно бути стратегічне планування, яке враховує визначення потреб персоналу, розвиток їх кар'єрних шляхів та найбільш ефективне управління фаховими здібностями підлеглих. Активізація процесів мотивації та заохочення сприятиме постійному удосконаленню системи мотивації, яка враховує як організаційні, так і особистісні потреби військовослужбовців. В свою чергу це призведе до розвитку кар'єри, створенню можливостей для підвищення персоналу відповідно до їх індивідуальних цілей, амбіцій та можливостей. Для визначення рівня підготовленості необхідна ефективна система оцінки роботи персоналу, вона повинна бути заснована на чітких критеріях і стандартах.

Навчання та розвиток персоналу в сучасному військовому управлінні є критично важливими для підвищення ефективності та адаптивності військових ресурсів вцілому. Розробка програм навчання та спрямування професійного розвитку, що відповідають індивідуальним потребам та цілям персоналу, вимагає комплексного підходу та глибокого розуміння як загальних, так і специфічних вимог військової служби. Сучасні програми навчання повинні враховувати усі складові даного процесу, як то базові військові навички, так і спеціалізовані компетенції. Необхідно, щоб ці програми були гнучкими та адаптованими до швидко змінюваного військового середовища. Це означає, що навчальні програми мають постійно оновлюватися, відображаючи новітні технологічні тенденції, зміни у тактиці ведення бойових дій, а також сучасні управлінські та лідерські підходи.

Ключовим елементом в розробці ефективних програм навчання є індивідуальний підхід. Кожен військовослужбовець має свій унікальний набір навичок, досвіду та кар'єрних цілей, і програма повинна пропонувати можливості для розвитку в цих напрямках. Це може включати індивідуальні чи спеціалізовані курси, або інші форми навчання, які допоможуть кожному військовослужбовцю досягти свого максимального потенціалу. Також важливо враховувати психологічні аспекти навчання та розвитку. Військова служба часто пов'язана з високим рівнем стресу та емоційного навантаження, тому програми повинні інтегрувати елементи психологічної підтримки та розвитку емоційного інтелекту. Це допоможе військовослужбовцям не тільки ефективно виконувати СБЗ, але й підтримувати психологічне здоров’я.

Розглядаючи НГУ в контексті військової структури, ключовою є розробка лідерських програм, адже військове лідерство вимагає не тільки стратегічного мислення та вміння приймати рішення в умовах невизначеності, але й здатності вести за собою людей, мотивувати та розвивати їх. Ці навички можуть бути розвинені через спеціальні лідерські тренінги та курси.

Тож можна стверджувати, що розробка програм навчання та професійного розвитку в НГУ є комплексним завданням, яке вимагає глибокого розуміння потреб персоналу, сучасних військових вимог та психологічних особливостей військової служби. Ефективні програми повинні бути гнучкими, адаптивними та спрямованими на розвиток індивідуального потенціалу кожного військовослужбовця.

Забезпечення балансу між службою та особистим життям є нагальною складовою управління персоналом, особливо в НГУ, де вимоги до дисципліни та професійних обов'язків часто є дуже високими. Це питання набуває особливої актуальності, оскільки військова служба вимагає тривалої відсутності вдома, регулярних переведень, а також передбачає участь у війні в різних регіонах держави та в різних якостях. Також, збалансованість необхідна для забезпечення психологічного благополуччя та високої продуктивності військовослужбовців, коли персонал відчуває, що їхні особисті потреби та інтереси поважають, вони, як правило, більш мотивовані та задоволені своєю роботою та службою. З іншого боку, ігнорування потреб у балансі може призвести до професійного вигорання, зниження морального духу та навіть до втрати кваліфікованих кадрів. Необхідно визнавати важливість цього балансу та постійно розробляти відповідні стратегії його підтримки. Це може бути розробка гнучких графіків службового навантаження, де це можливо, надання додаткових відпусток або вихідних днів для сімейних подій, вирішення соціальних потреб, а також забезпечення доступу до психологічної підтримки та консультування.

Також значущим є забезпечення підтримки сімей військовослужбовців, особливо коли військові залучені до довгострокових відряджень для виконання СБЗ. Сімейні програми підтримки, соціальні заходи та забезпечення комунікаційних засобів для підтримки зв'язку з сім'ями можуть відігравати суттєву роль у підтримці морального духу та загального благополуччя персоналу.

Однак, слід розуміти, що військова служба має свої унікальні вимоги, і повне досягнення балансу між роботою та особистим життям може бути складним. Проте, намагання досягти цього балансу є прогресом у забезпеченні ефективності та стійкості військових кадрів, військове керівництво повинно приділяти достатньо уваги вирішенню даного питання, розробляючи програми, які підтримують як професійний розвиток, так і особисте благополуччя підлеглого персоналу.

Зворотний зв'язок та комунікація є вирішальними елементами у ефективному управлінні військовим персоналом, де ці грані набувають особливої важливості через строгі ієрархічні структури та необхідність чіткого виконання обов'язків. Ефективні канали комунікації сприяють не тільки поліпшенню продуктивності, але й розвитку кар'єри та відкривають можливості для професійного росту. У військових структурах, де дисципліна та точне виконання розпоряджень є ключовими, зворотний зв'язок має бути чітким, конкретним та об'єктивним. Це дозволяє військовослужбовцям точно розуміти вимоги та очікування щодо їхньої роботи та поведінки, а також отримувати відповідну інформацію про їхні досягнення та напрямки їх поліпшення. Залучення військовослужбовців у процес зворотного зв'язку наголошує на тому, що комунікація не повинна бути односторонньою – персонал повинен мати можливість висловлювати свої думки, ідеї та занепокоєння, такий підхід сприяє створенню атмосфери відкритості та довіри.

Використання сучасних комунікаційних технологій може значно підвищити ефективність процесу зворотного зв'язку. Електронні системи управління, мобільні додатки та інші цифрові інструменти дозволяють забезпечувати швидке та ефективне спілкування, а також можуть використовуватися для систематичного збору та аналізу зворотного зв'язку. Процес зворотного зв'язку повинен також інтегруватися в систему оцінки продуктивності та планування кар'єри. Регулярне оцінювання, що базується на об'єктивному та конструктивному зворотному зв'язку, може визначати напрямки для професійного розвитку та підготовки. Такий підхід допомагає військовослужбовцям розуміти, як вони можуть досягти професійного зростання та реалізувати свій потенціал в підрозділі. Військова служба часто супроводжується високим рівнем стресу, тому підходи до зворотного зв'язку та комунікації повинні бути відповідно адаптовані, щоб забезпечити підтримку та зберегти позитивний моральний дух.

Ефективні канали зворотного зв'язку та комунікації є фундаментальними для забезпечення продуктивності, кар'єрного росту та професійного розвитку у військовій структурі, вони дозволяють створювати середовище, в якому персонал відчуває себе цінним та залученим, а також сприяють постійному покращенню та розвитку як індивідуально, так і на організаційному рівні.

Ефективне управління персоналом в умовах високого стресу та невизначеності є важливим для успішного ведення бойових дій та проведення військових операцій. В цих умовах традиційні методи роботи керівників з управління персоналом часто виявляються недостатніми, оскільки вони не завжди здатні адаптуватися до швидких змін у зовнішньому середовищі та до високого рівня динаміки ситуацій.

Наукові дослідження в області управління та психології підкреслюють, що в умовах високого стресу та невизначеності критичною стає здатність лідерів швидко адаптуватися до змінюваних обставин, це гнучке переосмислення стратегій, готовність до зміни планів відповідно до нових даних та здатність управляти ризиками в умовах обмеженої інформації. Ефективне керівництво в таких ситуаціях також вимагає високого рівня емоційного інтелекту, оскільки лідер повинен зберігати спокій, об'єктивно оцінювати ситуацію та забезпечувати моральну підтримку своїм підлеглим.

Окрім адаптивності та емоційної стійкості, для ефективного керування у таких умовах необхідна здатність до інноваційного мислення, що об’єднує розробку творчих рішень та використання нетрадиційних підходів у вирішенні проблем. В умовах стресу та невизначеності досить часто чіткі та звичні рішення недієві, тому креативність та інноваційний підхід мають вирішальне значення. Розвиток ефективної комунікації у стресових ситуаціях дозволяє забезпечити чіткий та своєчасний обмін інформацією між усіма учасниками процесу. Керівники повинні бути здатні не тільки передавати інструкції, але й підтримувати зворотний зв'язок, адекватно реагувати на доповіді та питання підлеглих, надавати їм допомогу. Ефективна робота команди, здатність до швидкого обміну інформацією та координації дій є ключовими для прийняття рішень у складних умовах. Розвиток навичок командної роботи, лідерства та взаємодії в команді може підвищити ефективність прийняття рішень на всіх рівнях військового управління.

Ефективне керування у стресових ситуаціях вимагає комплексного підходу, який поєднує адаптивність, емоційний інтелект, інноваційне мислення та ефективну комунікацію. Розвиток цих навичок та здібностей є важливим для забезпечення ефективності управління у складних умовах, що є характерними для бойових дій та інших кризових ситуацій.

Використання інноваційних підходів у сучасному військовому управлінні персоналом та впровадження інноваційних технологій і методик є необхідним кроком для підвищення ефективності та оптимізації процесів організації праці керівників з управління персоналом в органах військового управління та військових частинах НГУ. Розвиток технологій пропонує нові можливості для покращення управління персоналом, охоплюючи підготовку, навчання та оцінку продуктивності.

Сучасні технології, як-то штучний інтелект, автоматизоване навчання, аналітика даних різної величини та повноти, можуть значно покращити процеси відбору та залучення військового персоналу, дозволяючи автоматизувати багато процесів та забезпечити більш об'єктивний та ефективний підбір кандидатів. Використання алгоритмів для аналізу даних кандидатів може допомогти виявити найбільш перспективних претендентів з точки зору їхніх навичок, досвіду та потенціалу. У сфері підготовки, навчання та розвитку персоналу, використання інноваційних технологій, таких як віртуальна та доповнена реальність, забезпечує більш ефективний та практичний досвід навчання. Ці технології дозволяють створювати реалістичні тренувальні сценарії, які сприяють кращому засвоєнню навичок та підготовці до реальних викликів військової служби.

Враховуючи стрімкий розвиток технологій та їх вплив на всі сфери життя, необхідність впровадження сучасних технологій та методик у військовому управлінні персоналом є актуальною. Це вимагає не лише інвестицій у технологічні рішення, але й розвитку відповідних навичок та знань серед керівного складу, щоб вони могли ефективно використовувати ці інструменти для досягнення організаційних цілей. Такий підхід не тільки сприятиме покращенню процесів управління персоналом, але й загалом забезпечить більшу адаптивність та готовність НГУ до сучасних викликів.

Висновок. Результати дослідження підкреслили важливість і потребу в удосконаленні організації діяльності керівників з управління персоналом в НГУ. Було виявлено, що попри наявність сильних сторін в існуючій системі, існують значні прогалини та недоліки, які потребують систематичного підходу до їх вирішення. Особливо це стосується необхідності зміцнення ідейної бази серед військовослужбовців, а також розробки та впровадження інноваційних підходів до управління персоналом.

Аналіз наукових джерел та досвіду вказує на можливість значного підвищення ефективності через застосування сучасних методів управління персоналом, об’єднуючи мотиваційні стратегії, розвиток корпоративної культури та лідерства. Принциповою є інтеграція цих підходів в щоденну діяльність військових частин, що дозволить забезпечити більш високий рівень залученості серед особового складу.

Висновки та рекомендації дослідження надають чіткий напрямок для подальшого вдосконалення системи управління персоналом в НГУ. Вони складаються не тільки впровадження конкретних інструментів та технологій, але й розвиток загальної стратегії управління, що враховує специфіку військової служби та сучасні виклики.

Для реалізації висунутих пропозицій необхідна активна участь керівництва на всіх рівнях, готовність до змін та впровадження інновацій, а також забезпечення необхідних ресурсів для реформування. Систематичний моніторинг та оцінка впроваджених змін дозволять коригувати процес управління, адаптуючи його до змінних умов та нагальних потреб.

У підсумку, реалізація рекомендацій, виходячи з проведеного дослідження, сприятиме підвищенню ефективності управління персоналом, зміцненню обороноздатності та безпеки держави, а також забезпеченню стійкого розвитку НГУ, як значущої складової системи безпеки і оборони держави.

References:

1.(14). Доктрина з планування розвитку в Національній гвардії України: наказ Командувача НГУ від 01.03.2023 року №150. (позначка військової публікації: ВКП НГУ 5-00(06).01). URL: https://ngu.gov.ua/wp-content/uploads/2023/03/vkp-ngu-5-0006.01-doktryna-z-planuvannya-rozvytku-v-ngu

Про Дисциплінарний статут Збройних Сил України: Закон України від 24.03.1999 № 551-XIV *Відомості Верховної Ради України.* 1999 р. № 22. URL: https://zakon.rada.gov.ua/laws/show/551-14#Text (дата звернення: 09.01.2024).

Єрьоменко Е. (2014). Військово-патріотична програма та прикладний хортинг. *Теорія і методика хортингу*. 2014 р. № 1. С.10–19. URI: https://university-edu.science/handle/123456789/124

Мулява В., Богайчук В. (2020). Проблеми та шляхи удосконалення військово-патріотичного виховання і мотивації молоді до служби у Збройних силах України. *Вісник НУОУ*. 2020 р. № 2. С 68–74. DOI: https://doi.org/10.33099/2617-6858-2020-55-2-68-74

Пашкова О.О. (2019). Удосконалення військово-патріотичного виховання курсантів ВВНЗ в умовах збройної агресії проти України. *Воєнно-історичний вісник*. 2019 р. № 3 (33). С. 38–53.

Макух-Федоркова І. (2021). Роль соціальних медіа в сучасних міжнародних конфліктах. Міжнародні конфлікти у сучасному світі: від регіонального до глобального суперництва. праці 5 міжнар. наук. конф. (Львів, 2021 р.). Львів, 2021. С. 87–91. URL: https://www.ispc.org.ua/wp-content/uploads/2021/12/Conference-proceedings-12-2021.pdf#page=87

Набока С. (2022). Еволюція інформаційних технологій в історії людства та інформаційний вплив на свідомість населення в ході військових конфліктів. *Вісник науки та освіти.* 2022 р. № 3. С. 206–220.

Драбюк С. (2022). Пропаганда та її види. Шляхи протидії пропаганді. *Аналітично-порівняльне правознавство*. 2022 р. № 1. С. 153–157. DOI: https://doi.org/10.24144/2788-6018.2022.01.28

Шульська Н. М., Зінчук Р. С. (2022). Медіаманіпуляції в умовах російсько-української війни (на прикладі локальних ЗМІ). *Південний архів (філологічні науки)*. 2022 р. №90. С. 68–76. DOI: https://doi.org/10.32999/ksu2663-2691/2022-90-9

Усаченко О. О. (2022). Теоретичний аналіз феномену військового лідерства. *Публічне урядування.* 2022 р. № 5 (33). С. 109–113.
Заруба О. (2019). Лідерство у вищих військових навчальних закладах: моделі та програми підготовки. *Інформаційна безпека людини, суспільства, держави*. 2019 р. № 3 (27). С. 93–103. URL: https://journals.uran.ua/ispss/article/view/196127
Алещенко В. (2022). Психологічний континуум лідерства в організаційній культурі військового керівника. *Вісник НУОУ*. 2022р. №3. С. 5–12. DOI: https://doi.org/10.33099/2617-6858-2022-67-3-5-12
Севрук І., Соколовська Ю. (2022). Морально-етичні аспекти діяльності цивільних та військових на території країни, що зазнала військової агресії: український досвід. Серія філософсько-політологічні студії. *Вісник Львівського університету.* 2022 р. № 41. С. 78–87. URL: http://www.fps-visnyk.lnu.lviv.ua/archive/41_2022/11.pdf
14.(1). Доктрина з планування розвитку в Національній гвардії України: наказ Командувача НГУ від 01.03.2023 року №150. (позначка військової публікації: ВКП НГУ 5-00(06).01). URL: https://ngu.gov.ua/wp-content/uploads/2023/03/vkp-ngu-5-0006.01-doktryna-z-planuvannya-rozvytku-v-ngu

DOI 10.5281/zenodo.10820541

UDC 351.863(477)»364»

CHAPTER 7.

ANALYSIS OF THE ECONOMIC ASPECTS OF ENSURING THE NATIONAL SECURITY OF UKRAINE IN THE CONDITIONS OF WAR

Sergii V. IVANOV

Doctor of Economic Sciences, Professor,

General Director of LLC «Alcohol and non-alcoholic plant «Dnepr»,

Associate Member of the National Academy of Sciences of Ukraine

(St. Sviatoslav Khrabroho, 12 Dnipro, 49000, Ukraine)

ivanovsv@abkdnipro.com

https://orcid.org/0000-0002-1205-3797

Hanna V. RAZUMOVA

Doctor of Economic Sciences, Associate Professor,

Professor of the Department of Marketing and Business Administration,

SHEI «Priazovsky State Technical University»

(St. Gogolya, 29, Dnipro, 49000, Ukraine)

anna.raz888@gmail.com

https://orcid.org/0000-0003-4432-4050

Summary. The purpose of the study is to analyze the economic aspects of ensuring the national security of Ukraine. Factors affecting national security are analyzed. The evolution of views on national security is considered. The aspects that must be taken into account when developing an effective national security policy, adequate to the challenges and threats of the beginning of the 21st century in the context of globalization, are defined. The economic component of national security is considered in detail and the indicators characterizing it are analyzed.

Keywords: national security, economic security, martial law, national economy, geoeconomics, indicators of economic development.

АНАЛІЗ ЕКОНОМІЧНИХ АСПЕКТІВ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВІЙНИ

Анотація. Метою дослідження є аналіз економічних аспектів забезпечення національної безпеки України. Проаналізовано чинники, що впливають на національну безпеку. Розглянуто еволюцію поглядів на національну безпеку. Визначено аспекти, які необхідно врахувати при розробці ефективної політики національної безпеки, адекватної викликам та загрозам початку XXI століття у контексті глобалізації. Детально розглянуто економічну складову національної безпеки та проаналізовано показники, що її характеризують.

Ключові слова: національна безпека, економічна безпека, воєнний стан, національна економіка, геоекономіка, показники економічного розвитку.

Вступ. Стрімкі зміни в Україні й у всьому світі наприкінці XX – початку XXI століття, зокрема стан суспільства та державних інститутів, зміни в системі міжнародних відносин зумовили широкий інтерес до політики національної безпеки. Становлення такої політики насамперед пов'язане з питаннями пошуку національної ідентичності і, відповідно, визначенням національної стратегії розвитку країни, а також з дуже суперечливими процесами глобалізації, що відбуваються у світі.

Слід зазначити, що безпосередніми чинниками, які впливають на національну безпеку є демократизація, економізація та інформатизація.

Метою дослідження є аналіз економічних аспектів забезпечення національної безпеки України.

Чинники, що впливають на національну безпеку

Демократизація сучасного світу безповоротно змінює ієрархію основних об'єктів національної безпеки. На перше місце в цій ієрархії об'єктивно виходить особистість, на друге – суспільство, яке відтісняє державу на третє місце та робить її насамперед інструментом захисту своїх інтересів та інтересів особистості. Країна, яка претендує на помітну роль у світових відносинах сьогодні змушена дотримуватися цієї ієрархії об'єктів національної безпеки.

Демократизація, що йде іноді непослідовно і суперечливо, нікому не дає можливості безкарно зневажати демократичні норми та процедури, ігнорувати інтереси та права людини. Жодна держава сучасного світу не може собі дозволити одну політику всередині своїх кордонів та принципово іншу – за її межами. Саме таку політику, на нашу думку, проводить РФ, говорячи своїм громадянам про гуманні цілі розпочатої війни й при цьому обстрілюючи українські міста та села.

Економізація, що неухильно веде до формування єдиного світового економічного простору, робить нежиттєздатними моделі національної безпеки, засновані на ізоляціонізмі, а інтеграцію в цей простір – єдино можливим способом ефективного захисту національних інтересів. Відмова від інтеграції означає неможливість повноцінного економічного розвитку. А саме такий розвиток і є ключовою передумовою забезпечення національної безпеки. Жодна країна не може стати конкурентоспроможною, не ставши частиною світового економічного простору. Цей фактор також визначає пріоритетність геоекономічних механізмів забезпечення національної безпеки в порівнянні з геополітичними та геостратегічними, оскільки саме геоекономіка стає пріоритетом світового розвитку.

Нагадаємо, що геоекономіка – це наукова дисципліна, що вивчає економічну ситуацію в тій чи іншій країні і, спираючись на різні показники (її географічне розташування, історичний розвиток, культуру), визначає рівень економічного розвитку цієї країни та її місце у світовій політиці, на відміну від останньої, що бере до уваги лише рівень економічного впливу. Геоекономіка тісно пов'язана з іншими соціальними та суспільними науками, тому також стикається з геополітикою, вивченням глобалізації.

Як політична стратегія геоекономіка – це нова геополітика (геополітична економіка), яка розробляє стратегію підвищення впливу держави з позицій її економічної могутності та забезпечує досягнення зовнішньополітичних цілей, світової чи регіональної могутності економічним шляхом *(Wikipedia, 2024)*.

Інформатизація, що формує єдиний світовий інформаційний простір, створюючи глобальне мережеве суспільство, відкриває громадянам охоплених нею країн доступ до всіх матеріальних і духовних благ, множить інтелектуальний ресурс, а відтак і всі інші ресурси, сприяючи сталому розвитку, досягненню благополуччя та безпеки особистості та суспільства. З іншого боку, інформаційні технології не є абсолютним благом: вони створюють нові можливості для контролю та маніпуляції масовою свідомістю у внутрішній політиці та нові ефективні засоби міждержавного протистояння, а отже, і нові загрози національній безпеці.

На сучасному етапі світового розвитку глобалізація створює переваги для найбільш розвинених у соціально-економічному та технологічному сенсі країн (США, країн Євросоюзу, Японії), що веде до зростання розриву між ними та державами, що розвиваються. З іншого боку, саме ці країни внаслідок своєї розвиненості та накопиченого багатства, способу життя, цінностей та стереотипів поведінки стали в умовах глобалізації та створення мережевого суспільства найбільш уразливими для нових викликів та загроз. Повсюдне поширення телебачення, що зробило загальнодоступними для бідних країн образи й стандарти недосяжно

багатого західного суспільства, стимулювало в деяких бідних країнах (насамперед мусульманського світу) хвилю антизахідних настроїв, зокрема і міжнародного тероризму.

У результаті світ на початку XXI століття зіткнувся з новим глобальним безпековим викликом. В умовах глобалізації та розпаду сформованого після Другої світової війни світового порядку внаслідок розпаду СРСР та біполярного світу відбулося різке падіння рівня керованості міжнародними процесами.

Колишні системи та механізми міжнародної безпеки виявилися неефективними, різко зросла регіональна та частково глобальна нестабільність. Це стимулювало те, що національна безпека виявилася тісно пов'язаною з міжнародною безпекою.

Міжнародний вимір національної безпеки, який і раніше ніким не заперечувався, багаторазово зріс. Відтепер будь-яка держава, у тому числі й Україна, може почуватися у відносній безпеці лише в умовах формування нового, більш справедливого світового порядку, що відповідає інтересам усіх країн світової спільноти.

Процеси глобалізації, з одного боку, розмивають класичний національний суверенітет, з іншого, – сприяють підвищенню рівня національної самосвідомості народів. Усе це впливає на проблеми забезпечення як національної, так і міжнародної безпеки. Таким чином, наслідки глобалізації для забезпечення національної та міжнародної безпеки є вельми суперечливими. Вона створює як нові можливості для розвитку та процвітання різних країн, так і нові, вкрай небезпечні, виклики та загрози.

Для України, що продовжує перебувати в стадії соціально-економічної трансформації і водночас зберігає з об'єктивних причин наступність своїх як регіональних, так й глобальних інтересів, усі ці положення є особливо важливими і актуальними.

На сьогодні, а також у найближчому майбутньому, стан справ у світовій політиці такий, що лідером глобалізації є США. Саме вони мають найбільший вплив на формування нового світового порядку. Майже всі проблеми міжнародної безпеки неможливо вирішити без активної участі США. Ця обставина робить для України співпрацю зі США життєвонеобхідною, оскільки в умовах вищезгаданої взаємозалежності міжнародної та національної безпеки забезпечити останню без тісної взаємодії з лідером глобалізації навряд чи можливо.

Гострота та специфіка змісту та сенсу цього виклику обумовлена також новими підходами США до своєї безпеки, до міжнародних відносин та міжнародного права загалом. Важливим етапом у концептуальному осмисленні політики національної безпеки стало ухвалення Закону України «Про національну безпеку України» *(Verkhovna Rada of Ukraine, 2018)*, який набув чинності у 2018 році.

Протягом 2019–2020 років велася робота над Концепцією зовнішньої політики України. Так, під час першого етапу (2019 рік) були проаналізовані основні регіональні напрями зовнішньої політики України, двосторонні відносини із США, Російською Федерацією та КНР, а також місце України в євроатлантичних структурах безпеки. Деякі з цих питань були додатково опрацьовані протягом 2020 року.

Другий етап (2020 рік) був присвячений тематичним напрямам (економічна, енергетична, публічна дипломатія, питання безпеки тощо), а також підготовці фінальних рекомендацій.

Пандемія коронавірусу призвела до різкого й неочікуваного падіння рівня світової економіки, уповільнення або припинення торговельних зв'язків, активізувала протистояння США і Китаю, стала каталізатором перегляду інвестиційної і торговельної політики країни з точки зору усунення монополізму (насамперед у сфері виробництва медичних товарів), фактичному банкрутству цілих галузей транспорту й туризму. Активізувались і політичні процеси, пов'язані зі спробами пошуків винних в економічних проблемах, пов'язаних з пандемією, а також ростом популізму.

Проте все ж таки підготовлений документ дозволив реалістично визначити пріоритети зовнішньої політики України, які є необхідними умовами захисту національних інтересів країни, та шляхи їх досягнення. У документі визначено місце української держави у світі, її сприйняття з боку інших держав, аналіз поточних світових тенденцій, усвідомлення викликів та перспектив у різних сферах.

У цьому документі визначено, що, відповідно до класифікації Міжнародного валютного фонду, Україна належить до групи Emerging and Developing Europe, до якої увійшли ще 16 країн (Албанія, Білорусь, Боснія та Герцеговина, Болгарія, Косово, Молдова, Північна Македонія, Польща, Румунія, Росія, Сербія, Туреччина, Україна, Угорщина, Хорватія, Чорногорія) – як членів ЄС, так і членів Східного партнерства.

ВВП України у 2019 році становив 150 млрд дол. США, що складало 0,3% від світового ВВП. Посідаючи 32-ге місце у світі за кількістю населення та 47-ме місце за розміром території, маючи багаті природні ресурси, Україна посідає лише 55-те місце у світовій торгівлі, що, за висновками міжнародних організацій та фінансових інституцій, свідчить про неефективне використання наявного потенціалу та можливостей.

Рівень ВВП на душу населення в Україні є передостаннім серед держав Європи. Обтяжувальним фактором у документі визнано вимушені високі оборонні витрати, спричинені агресією РФ (5% ВВП, 14 місце у світі), обнадійливим фактором – високий рівень освіти та доступу до Інтернету (29 місце у світі).

Водночас у документі зазначено, що Україна є відповідальним членом міжнародних організацій, довгий час посідала провідне місце серед держав-контрибуторів до операцій з підтримки миру, є одним із лідерів серед країн-експортерів зерна, продукції металургійної та авіапромисловості, оборонного співробітництва та торгівлі озброєнням.

Також у документі зазначено, що досвід, набутий за роки російсько-українського конфлікту, зокрема щодо протидії новим викликам, гібридним загрозам, кібератакам та інформаційним операціям, є важливим фактором безпекового та політичного співробітництва з країнами світу *(Haber Ye., Korsunskyi S., Shelest H. (ed.), 2020).*

Еволюція поглядів на національну безпеку

Якщо проаналізувати еволюцію поглядів на національну безпеку, то зрозуміло, що з часом вони суттєво змінювалися.

Так, з середини 30-х до кінця 80-х років як основна модель вирішення теоретичних та практичних проблем безпеки виступала парадигма державної безпеки, у межах якої всі проблеми безпеки країни вирішувалися на основі пріоритету інтересів держави – основного суб'єкта та об'єкта забезпечення безпеки.

З кінця 80-х – початку 90-х років почалося становлення нової парадигми національної безпеки, що охоплює в порядку пріоритетності безпеку особистості, суспільства та держави.

У сучасному періоді дослідження проблем безпеки характеризуються, з одного боку, усебічною розробкою концепцій, основ теорії та політики національної безпеки, а з іншого – дослідженням методологічних та концептуальних проблем безпеки особистості, суспільства та держави. Також досліджуються такі важливі аспекти безпеки, як інформаційні, військові, геополітичні, геоекономічні, енергетичні, культурологічні, гуманітарні, синергетичні, соціологічні, загальнотеоретичні та інші.

Важливими темами дослідження безпеки держави стали також політичні фактори та питання профілактики та деескалації конфліктів, а також протидії тероризму.

Особливо треба відзначити такі аспекти безпеки, як питання національної ідентичності та національних інтересів.

Західні дослідники проблем міжнародних відносин та безпеки представляють дві головні наукові школи («реалістичну» та «ідеалістичну»).

Представники першої школи (Х. Моргентау, К. Уолтц, Д. Коллінз тощо) говорять про безпеку з позиції влади, своєкорисливих інтересів держави (насамперед – із прагнення більшої безпеки). Інша школа (Д. Мітрані, Р. Кеоейн, Дж. Найя, Р. Бертон тощо) бачать основу безпеки у світі, який може бути досягнутий через задоволення потреб усіх націй.

Фішер Д., вважаючи, що обидва підходи мають частку істини й можуть бути об'єднані, вважає, що справжня безпека не може бути досягнута за рахунок інтересів інших держав. Що стосується робіт, за якими найбільш адекватно можна робити висновки про сприйняття становлення політики національної безпеки в Україні в останні 10-12 років західними країнами, то до них насамперед слід зарахувати книги З. Бжезинського, І. Валлерстайна, Ш.Г. Кісінджера, С. Хантінгтона та інших.

Узагальнюючи вищевикладене, можна зазначити, що політика національної безпеки України спрямована на захист національних інтересів і національних цінностей та їх примноження в контексті сталого демократичного розвитку з урахуванням глобальних, регіональних та національних умов.

Формування та здійснення національної безпеки забезпечують засоби та ресурси, суб'єкти та механізми реалізації політики безпеки, її головні напрями та принципи, етапи й умови її вироблення та реалізації.

Перед Україною стоїть завдання розробки новітньої ефективної політики національної безпеки, адекватної викликам та загрозам початку XXI століття у контексті глобалізації. Проте необхідно враховувати певні аспекти.

1. Проблему національної безпеки та її складових частин не можна розглядати лише з погляду інтересів поточного періоду; вона має тісно пов'язуватися з потребами та можливостями перспективного періоду. З іншого боку, формування національної безпеки та її складових не може бути застиглим за своїми підходами та формами, за методами практичної реалізації. Вони завжди повинні враховувати реальну ситуацію як загалом, так і в окремих сферах, а також найбільш імовірні тенденції розвитку.

2. У геостратегічному плані Україна розташована на просторах Європи, що є свого роду осьовим районом світової політики. Саме це створює передумови для здійснення за допомогою України геостратегічної місії рівноваги між Сходом та Заходом.

3. Розробки щодо забезпечення національної безпеки повинні доходити консенсусу, або принаймні мати досить широку й чітко виражену національну згоду (між окремими партіями, групами) з низки ключових питань, що стосуються вибору моделі соціально-економічного та суспільно-політичного розвитку країни, і синтезувати переваги народу та еліти щодо державного ладу, економічної системи та характеру взаємин із зовнішнім світом.

4. Сьогодні головні загрози життєвоважливим інтересам України надходять ззовні, вони є наслідком агресії РФ.

Виходячи з цього, пріоритети завдань національної безпеки України слід розставити, на нашу думку, у такий спосіб: перше місце посідає перемога у війні з РФ, тобто відновлення

територіальної цілісності, необхідність захисту всіх завоювань країни за роки незалежності від загрози ззовні, стримування зовнішньої агресії в подальшому та забезпечення життєвоважливих інтересів за межами національної території. Друге місце посідають внутрішньополітичні та соціальні завдання – захист прав і свобод особистості, побудова основ демократичного суспільства та держави. Третє місце – це забезпечення вільного та ефективного економічного розвитку, підвищення добробуту громадян.

5. Національні цілі та інтереси України – це одночасно й забезпечення суспільного розвитку, формування стратегічних завдань внутрішньої та зовнішньої політики країни.

За змістом вони є інтегрованим виразом життєвоважливих інтересів особистості, суспільства та держави. При цьому найважливішими мають бути інтереси людини. Так, головною метою політики в галузі національної безпеки слід вважати створення механізму, що забезпечує максимально сприятливі внутрішні та зовнішні умови для підвищення якості життя українських громадян на основі сталого демократичного розвитку, ефективних економічних процесів на основі ринкових відносин та захисту інтересів особистості, суспільства та держави від протиправних зазіхань, суспільно небезпечних діянь, соціальних конфліктів, надзвичайних ситуацій, спричинених стихійними лихами, аваріями та катастрофами, від довготривалих екологічних та інших загроз.

6. Будь-яка діяльність, у т.ч. й забезпечення національної безпеки України, пов'язана з використанням тих чи інших ресурсів, під якими можна розуміти як ресурси матеріальні, так й ідеальні. Проблема ресурсів має стати ключовою проблемою національної безпеки, оскільки з нею тісно пов'язані засоби її забезпечення.

Першоджерелом усіх ресурсів має стати інтелект, з яким пов'язана диверсифікація й розвиток всіх систем людської діяльності та створення нових способів (насамперед засобів) використання матеріалу й устаткування. Це могло б дати Україні найважливіші інтелектуальні переваги.

7. Окреслене бачення забезпечення національної безпеки потребуватиме нової ресурсної політики. Згідно з панівним на цей час натуралістичним підходом і в Україні, і у світі загалом, ресурси існують об'єктивно стосовно діяльності й повинні бути «втягнуті» ззовні в діяльність для забезпечення її безперебійного функціонування як вхідний матеріал («сировинні ресурси»), або інші важливі компоненти забезпечення («фінансові ресурси», «кадрові ресурси» тощо). Згідно з новими підходами, уявленнями про ресурсне забезпечення національної безпеки, основними для поняття «ресурсів» є межі цілеспрямованої людської активності. І ресурси слід розуміти як штучно-природні. Ресурсами стає щось тоді, коли з'являються можливості та способи використання цього в процесі якоїсь діяльності.

8. Сьогодні потрібні нові методи актуалізації ресурсів. Ресурси потрібні у процесі діяльності (та/або під час створення нових систем, що не існували раніше). Створення нових або кардинальне оновлення наявних систем виливається у створення нового способу використання матеріалу при перетворюваній (новій, інноваційній) діяльності (додатково або замість того матеріалу, який раніше використовувався). Після завершення процесу перетворень, коли нова система діяльності починає ефективно функціонувати, нові ресурси знову перетворюються на відомі, нормативно описані (сировина, технічні засоби, кадри тощо), які мають лише відновлюватися відповідно до «зносу» або безповоротного використання протягом усього терміну експлуатації цієї системи діяльності.

Нова ресурсна політика покликана забезпечити конкурентоспроможність України як держави, її національної економіки та окремих галузей економіки, вітчизняних приватних компаній, інноваційних систем тощо в глобальному світі, що є однією з головних передумов національної безпеки. Включаючись у процеси глобалізації, Україна має не лише реалістично оцінювати свій ресурсний потенціал, а й уміти ним управляти.

9. Відповідно, до вищезазначеного необхідні нові механізми та інструменти здійснення ресурсної політики, яка в умовах жорсткої конкуренції національних держав та інших суб'єктів (ТНК та інших) на світовій арені стане одним з головних напрямів політики національної безпеки.

10. Україна володіє природними багатствами, а за деякими з них посідає перші місця у світі. Але в країні немає дієвих концепцій, програм і проєктів використання всіх цих багатств, вони не включаються до господарського обігу, а отже, не є багатством, недостатньо сприяють розвитку України та добробуту її громадян.

11. Політика національної безпеки реалізується через відповідні процеси, перебіг яких пов'язаний із функціонуванням відповідних механізмів. Цими механізмами насамперед є різноманітні форми організації та процедури різних типів діяльності, що так чи інакше застосовуються в системі забезпечення національної безпеки.

12. Політика безпеки України має включати оцінку геополітичного, геостратегічного та геоекономічного становища країни; оцінку характеру реальних та потенційних загроз безпеці; визначення життєво важливих національних інтересів, стратегічних цілей та пріоритетів внутрішньої та зовнішньої політики країни; визначення засобів (ресурсів) забезпечення безпеки; механізми реалізації безпекової політики.

13. Кожному з етапів реалізації національних інтересів України відповідають свої оцінки перерахованих категорій і, відповідно, свій механізм реалізації такої політики. Складовими частинами національної безпеки є економічна, оборонна, зовнішньоекономічна,

геополітична, громадська, екологічна, інформаційна безпека та низка інших складових національної безпеки. Вони діють у єдиній системі, залежать один від одного та взаємодіють між собою.

Економічна складова національної безпеки

Розглянемо більш детально економічну складову національної безпеки в системі різноманітних факторів, що дестабілізують забезпечення національної безпеки України.

Особливе значення економічної безпеки держави обумовлено забезпеченням добробуту окремого індивідуума і сталим розвитком усієї нації. Процес глобального реформування економіки в нашій країні набуває соціальної орієнтації, призводить до необхідності розробки механізмів ефективної взаємодії всіх секторів економіки у вирішенні соціальних проблем, створення адекватної економічної та правової бази для розвитку суб'єктів країни.

Економічна безпека як тема теоретичних та прикладних досліджень, що виходять за рамки проблем оборонного сектора економіки, стала розроблятися в останнє десятиліття, оскільки саме в цей період особлива увага приділяється проблемі забезпечення національної безпеки держави, створенню конкурентоспроможного, незалежного від зовнішніх впливів господарського комплексу. Це зумовлено тим, що сучасна епоха характеризується глобальними змінами, що раніше здавалися непорушними. Зокрема, ще донедавна не передбачалося, що ринки інформації, фінансові, ринки трудових ресурсів тощо будуть настільки відкритими.

Західні дослідники розглядають економічну безпеку як процес забезпечення стабільної економічної політики. На їхню думку, захист національних інтересів, досягнення фінансової незалежності особливо важливі в умовах глобалізації. У зв'язку з цим, виняткового значення набуває вивчення структурного аспекту взаємодії національної економіки з глобальною економікою. Виникає необхідність аналізу у виборі підходу до проблеми забезпечення економічної безпеки країни на основі об'єктивної відтворювальної трансформації національної економіки в процес формування та розвитку світової економіки. Такий підхід особливо важливий у зв'язку з тим, що на цей час інтеграція України із світовим економічним співтовариством відбувається в умовах військового стану через агресію РФ.

Розглядаючи основи економічної безпеки необхідно зазначити, що під терміном «економічна безпека» розуміється спроможність національної економіки зберігати стійкість та невразливість до внутрішніх і зовнішніх загроз, забезпечувати високу конкурентоспроможність у світовому економічному середовищі, а також стале та збалансоване зростання.

Складові, що наведено у визначенні економічної безпеки є важливими критеріями оцінювання якісних параметрів національної економіки, стратегічної ефективності економічної політики держави в економічній сфері.

Виявлення загроз економічної безпеки та її складових частин має особливу актуальність в умовах різкого розширення та посилення потужності загроз, зумовлених повномасштабною агресією РФ проти України.

У перші місяці повномасштабної війни економічна безпека України значною мірою забезпечувалася накопиченими у довоєнний час резервами та запасом міцності, оперативною консолідацією зусиль суспільства на регіональному та місцевому рівнях, самоорганізацією та згуртованістю громадян України перед екзистенційною загрозою російської агресії, наданням безпрецедентної міжнародної підтримки.

З переходом російської агресії у форму затяжної війни на виснаження безпосередній вплив бойових дій на економіку посилився цілеспрямованими атаками на критичну інфраструктуру країни, виснаженням фінансових резервів населення та бізнесу, наростанням економічних диспропорцій, що сформувалися у воєнний період, застосуванням з боку ворога потенціалу різноманітних гібридних інструментів впливу.

Це актуалізує потребу здійснення цілеспрямованої політики держави щодо протидії комплексу ризиків і загроз економічній безпеці в умовах війни *(National Institute for Strategic Studies, 2023)*.

Основні ознаки класифікації видів економічної безпеки визначено Національним інститутом стратегічних досліджень. Так, ними є

- макроекономічна безпека;
- виробнича безпека;
- фінансова безпека;
- зовнішньоекономічна безпека;
- інвестиційно-економічна безпека;
- соціальна безпека;
- продовольча безпека.

На рис. 1 наведено основні складові перерахованих видів економічної безпеки в Україні в умовах воєнного стану.

Рисунок 1 – Основні складові макроекономічної безпеки в Україні в умовах воєнного стану

Наведені основні складові макроекономічної, фінансової, інвестиційно-інноваційної, виробничої, зовнішньоекономічної, соціальної та продовольчої безпеки (рис. 1-7) дозволяють сформувати уявлення про характер впливу війни на економічну безпеку України. За таких умов загроза може визначатися як потенційна подія, дія або обставина, яка може завдати шкоди, збитків у певній сфер, а ризик визначається як поєднання ймовірності та потенційного впливу загрози.

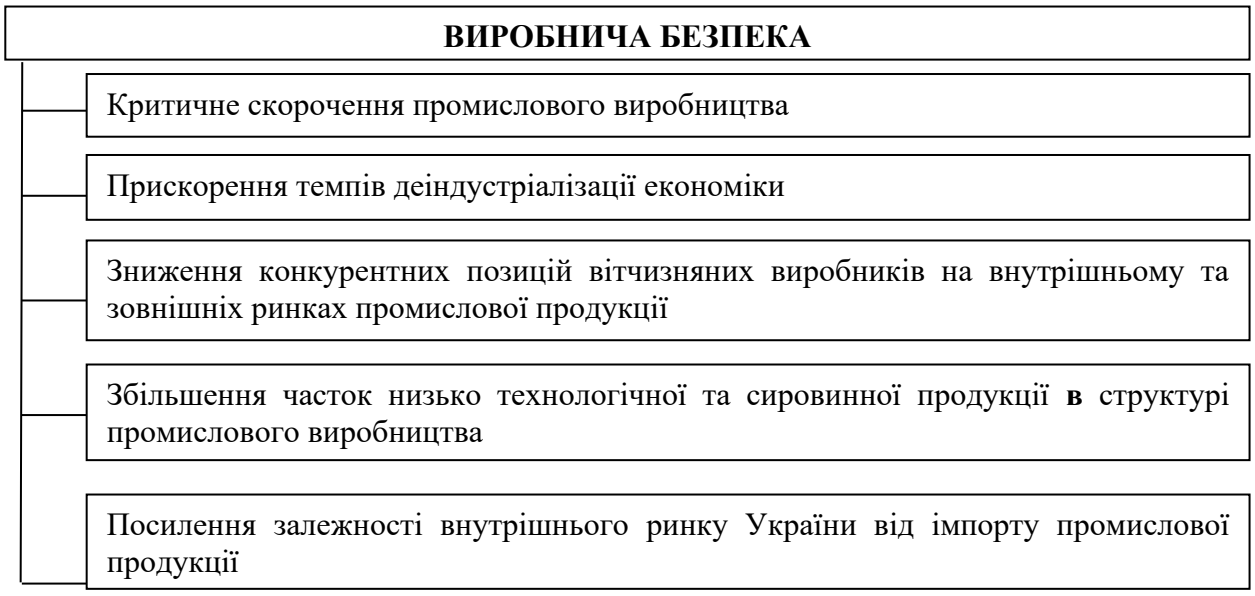


Рисунок 2 – Основні складові виробничої безпеки в Україні в умовах воєнного стану

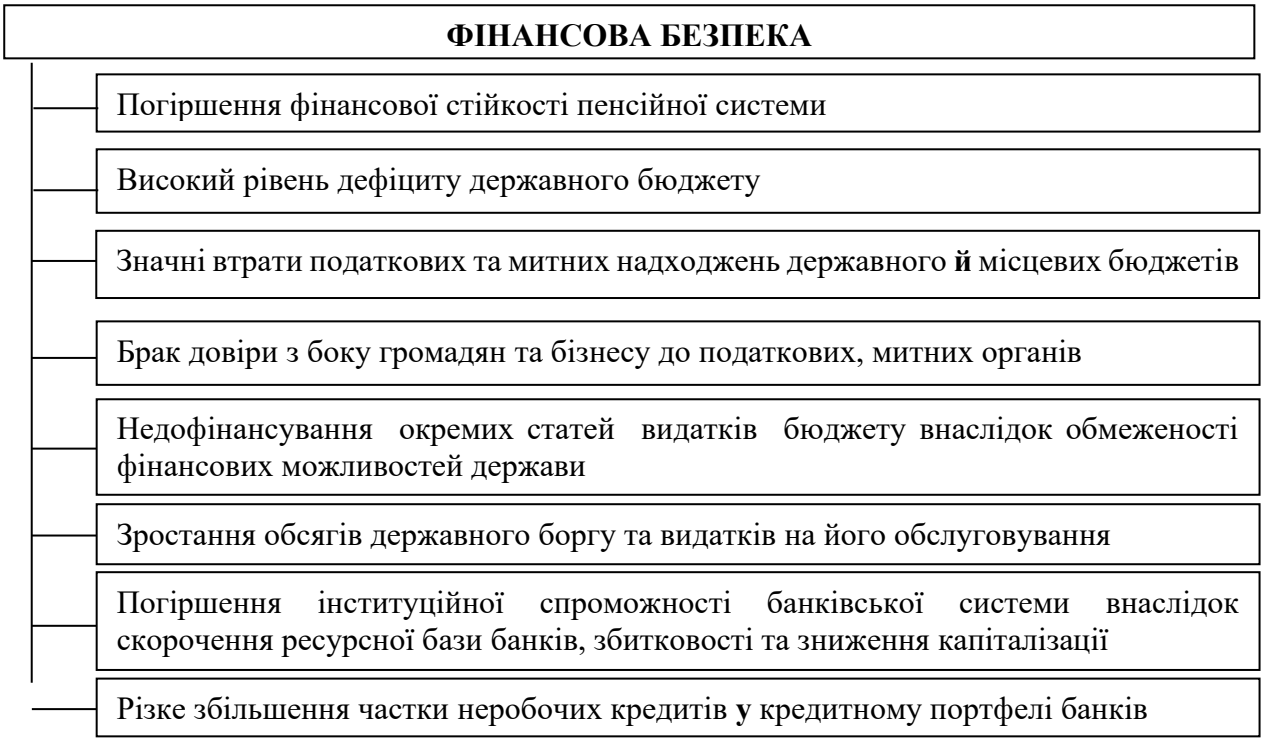


Рисунок 3 – Основні складові фінансової безпеки в Україні в умовах воєнного стану

Як було показано на рис. 1, до основних складових макроекономічної безпеки в Україні в умовах воєнного стану необхідно віднести різкий економічний спад унаслідок згортання ділової активності в умовах війни, неможливості ведення бізнесу в окремих регіонах країни в зоні бойових дій або в ризиковій зоні.

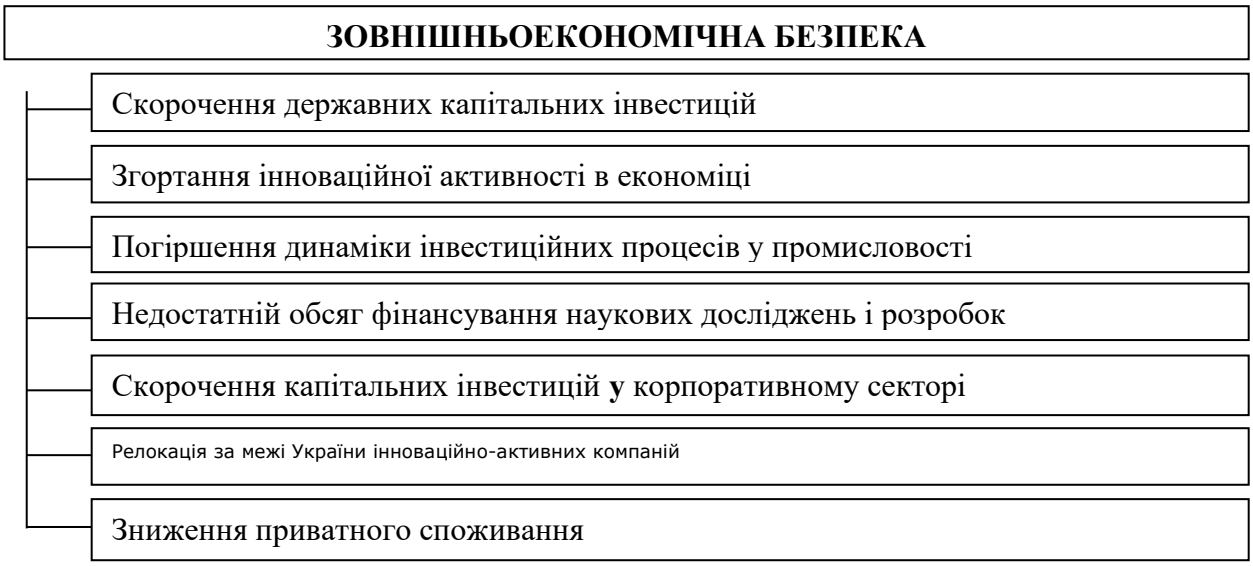


Рисунок 4 – Основні складові зовнішньоекономічної безпеки в Україні в умовах воєнного стану

ІНВЕСТИЦІЙНО-ІННОВАЦІЙНА БЕЗПЕКА

- Різкий економічний спад унаслідок згортання ділової активності в умовах війни, неможливості ведення бізнесу **в** окремих регіонах країни **в** зоні бойових дій або зоні ризику
- Відплив капіталу з економічної території України та релокація бізнесу за кордон
- Значне скорочення інвестиційної діяльності
- Критичне зниження обсягів кредитного фінансування основного капіталу, обігових коштів та інвестицій
- Зменшення трудового потенціалу внаслідок інтенсивних процесів міграції населення за кордон, значної частки ВПО, втрат цивільного населення внаслідок бойових дій
- Зростання індексу споживчих цін (інфляції)
- Зниження приватного споживання

Рисунок 5 – Основні складові інвестиційно-інноваційної безпеки в Україні в умовах воєнного стану

СОЦІАЛЬНА БЕЗПЕКА

- Суттєве погіршення соціально-економічного становища вразливих верств населення
- Суттєве зниження спроможності системи соціального захисту України виконувати свої функції
- Втрата можливостей зайнятості та поглиблення структурних диспропорцій на ринку праці
- Значне зниження добробуту та якості життя населення
- Погіршення доступу до кваліфікованої медичної допомоги
- Погіршення доступу до отримання соціальних послуг через нестачу фахівців з надання соціальних послуг
- Погіршення умов життя значних груп населення через руйнування житла та цивільної інфраструктури
- Масовий виїзд біженців за кордон
- Значне погіршення стану довкілля (включаючи воєнне забруднення), спричинене бойовими діями
- Збільшення навантаження на соціальну інфраструктуру та ринок праці густозаселених і традиційно праценадлишкових західних регіонів
- Стрімке зростання кількості ВПО

Рисунок 6 – Основні складові соціальної безпеки в Україні в умовах воєнного стану

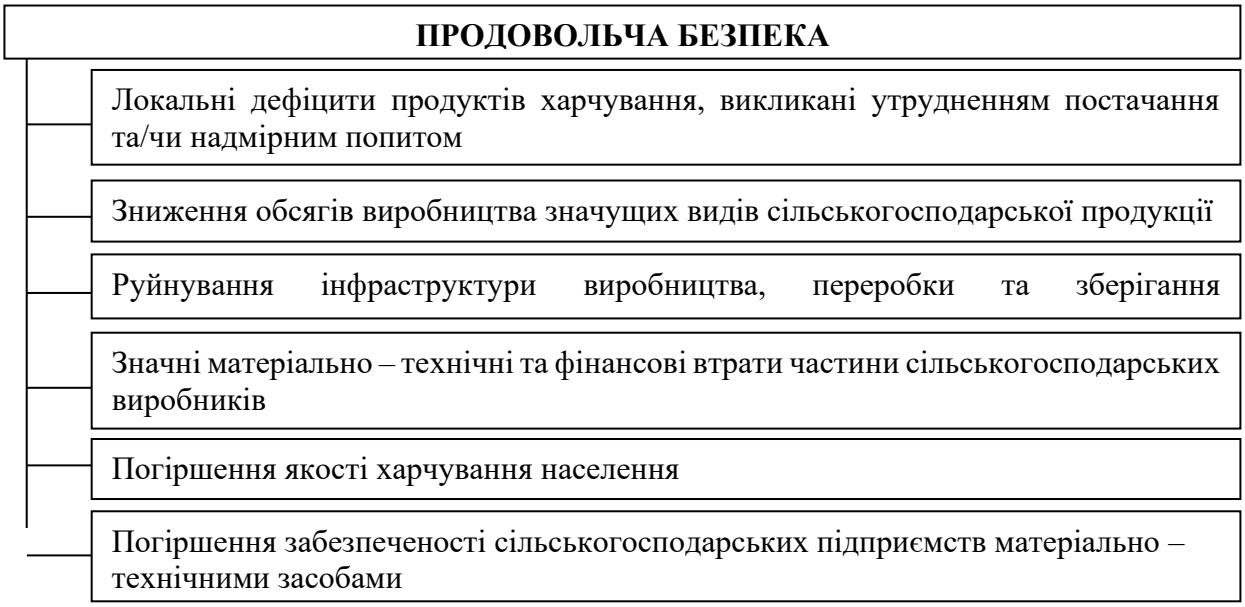


Рисунок 7 – Основні складові продовольчої безпеки в Україні в умовах воєнного стану

У табл. 1 наведено номінальний та реальний ВВП з 2012 по 2022 роки *(Minfin, 2024)*.

Таблиця 1 – Номінальний та реальний ВВП України в динаміці за 2012–2022 роки, млн грн

Роки	Номінальний ВВП (в фактичних цінах)	Реальний ВВП (в цінах попереднього року)	Відхилення (реальний від номінального)	
			Абсолютне, млн грн	Відносне, %
2012	1408889	1304064	-104825	-7.4%
2013	1454931	1410609	-44322	-3.0%
2014	1566728	1365123	-201605	-12.9%
2015	1979458	1430290	-549168	-27.7%
2016	2383182	2034430	-348752	-14.6%
2017	2982920	2445587	-537333	-18.0%
2018	3558706	3083409	-475297	-13.4%
2019	3974564	3675728	-298836	-7.5%
2020	4194102	3818456	-375646	-9.0%
2021	5459574	4363582	-1095992	-20.1%
2022	5191028	3865780	-1325248	-25.5%

За даними табл. 1 можна зробити висновок, що в країні спостерігається зниження реального ВВП майже на 25%. Після подій 2014 року в Україні аналогічний показник складав майже 27%. Тобто можемо зазначити, що події останніх десяти років, які були пов’язані з агресивними діями РФ, впливали на зниження реального ВВП, тобто погіршували стан економіки, знижали її конкурентоспроможність, інвестиційну привабливість тощо. РФ намагалася усунути з глобальних ринків свого потенційного конкурента в окремих сферах економічної діяльності (продовольчій, металургійній, енергетичній тощо).

У табл. 2 наведено перелік прямих іноземних інвестицій в Україну та з України за 2002–2023 роки *(Minfin, 2024)*.

За даними табл. 2 побудовано динаміку прямих інвестицій в Україну.

Дані табл. 2 та рис. 8 демонструють, що піки суттєвого зниження притоку інвестицій в Україну були обумовлені фінансовою кризою 2008–2009 років; кризою 2014 року через анексію Криму та окупацію частини Донбасу; пандемією 2020 року; повномасштабним вторгненням РФ в Україну у 2022 році.

Таблиця 2 – Прямі іноземні інвестиції в Україну та з України в динаміці за 2002–2023 роки, млн дол.

Роки	Прямі іноземні інвестиції в Україну		Прямі іноземні інвестиції з України		Відхилення (інвестицій в Україну від інвестицій з України)	
	млн дол. США	Приріст до попереднього року	млн дол. США	Приріст до попереднього року	Абсолютне, млн дол. США	Відносне, %
2002	693		-5		+698	
2003	1424	731	13	18	+1411	102.1%
2004	1715	291	4	-9	+1711	21.3%
2005	7808	6093	275	271	+7533	340.3%
2006	5604	-2204	-133	-408	+5737	-23.8%
2007	9891	4287	673	806	+9218	60.7%
2008	10913	1022	1010	337	+9903	7.4%
2009	4816	-6097	162	-848	+4654	-53.0%
2010	6495	1679	736	574	+5759	23.7%
2011	7207	712	192	-544	+7015	21.8%
2012	8401	1194	1206	1014	+7195	2.6%
2013	4499	-3902	420	-786	+4079	-43.3%
2014	410	-4089	111	-309	+299	-92.7%
2015	-458	-868	-51	-162	-407	-236.1%
2016	3810	4268	16	67	+3794	-1032.2%
2017	3692	-118	8	-8	+3684	-2.9%
2018	4455	763	-5	-13	+4460	21.1%
2019	5860	1405	648	653	+5212	16.9%
2020	-868	-6728	82	-566	-950	-118.2%
2021	6687	7555	-198	-280	+6885	-824.7%
2022	1152	-5535	529	727	+623	-91.0%
2023	1179	27	36	-493	+1143	83.5%

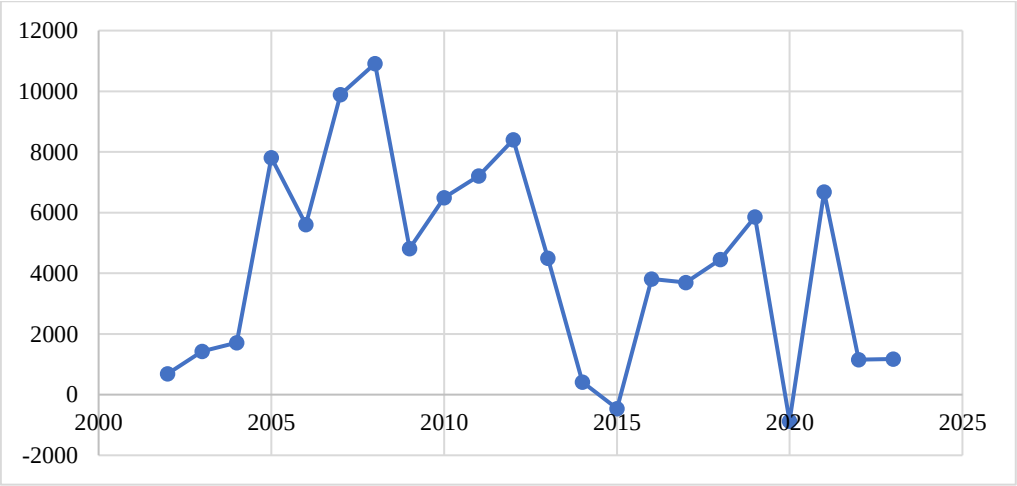


Рисунок 8 – Динаміка прямих іноземних інвестицій в Україну за 2002-2023 роки

У 2022 році спостерігалося найбільше зниження притоку інвестицій в Україну за двадцять попередніх років (на 5 535 млн дол. США).

На рис. 9 наведено динаміку іноземних інвестицій з України за 2002–2023 роки.

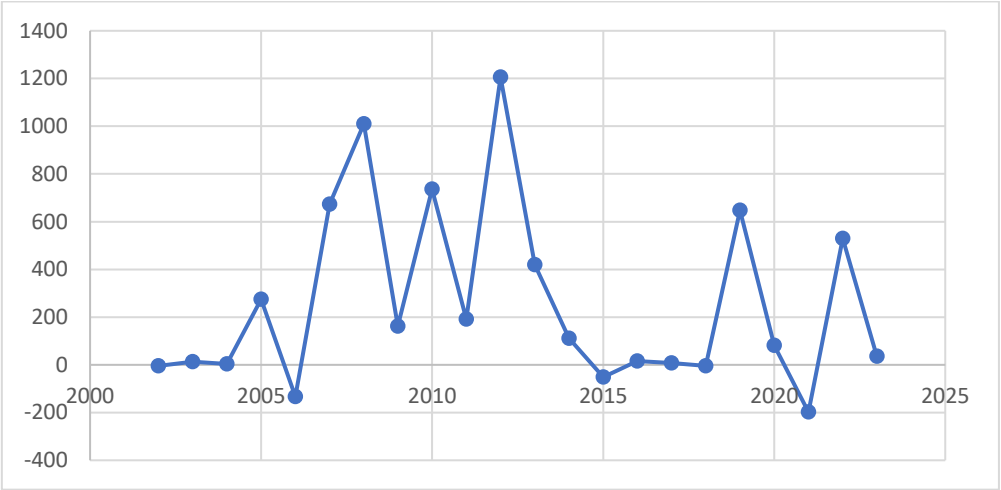


Рисунок 9 – Динаміка прямих іноземних інвестицій з України за 2002-2023 роки

Табл. 2 та рис. 9 демонструють нерівномірність відтоку іноземних інвестицій з України. Вони також характеризуються піками через вищезазначені кризи. Загальний обсяг інвестицій з України на порядок менший ніж притік.

Отже, наведені показники показують значне скорочення інвестиційної діяльності через війну в Україні.

У табл. 3 наведено перелік кредитів, наданих депозитними корпораціями (крім НБУ) за 2005–2023 роки *(National Bank of Ukraine, 2024)*.

За даними табл. 3 побудовано динаміку наданих кредитів комерційними банками.

На основі даних, наведених у табл. 3 та на рис. 10, можемо зробити висновок, що в Україні до 2014 року відбувалося нарощування кредитування суб'єктів ринкової економіки. Починаючи з 2014 року, ситуація як щодо загальних обсягів наданих кредитів, так і щодо

наданих кредитів терміном до 1-го року, почала кардинально змінюватися. Як правило, кредити терміном до 1-го року використовуються на фінансування обігових коштів.

Таблиця 3 – Кредити, надані депозитними корпораціями (крім НБУ) за 2005–2023 роки, млн грн

Роки	Усього	У тому числі		
		До 1 року	Від 1 року до 5 років	Більше 5 років
2005	1 663	991	672	…
2006	2 689	1 341	1 348	…
2007	5 932	2 823	2 626	484
2008	9 789	3 913	4 934	942
2009	14 014	8 659	4 001	1 354
2010	13 430	7 478	4 682	1 271
2011	16 441	9 274	5 953	1 214
2012	16 229	9 094	6 116	1 019
2013	19 317	11 056	7 247	1 015
2014	25 576	14 989	9 398	1 188
2015	15 564	9 377	4 372	1 815
2016	11 583	5 497	4 181	1 905
2017	10 936	4 805	4 086	2 046
2018	9 222	4 940	3 402	880
2019	9 577	5 554	3 248	774
2020	5 701	3 057	2 277	367
2021	9 644	6 095	2 451	1 098
2022				
липень	9 830	4 616	2 975	2 239
серпень	9 014	3 691	2 952	2 372
вересень	7 145	2 848	2 989	1 308
жовтень	7 120	2 953	2 873	1 294
листопад	6 656	2 579	2 796	1 281
грудень	6 809	2 814	2 724	1 272
2023				
січень	6 143	2 369	2 509	1 264
лютий	6 092	2 418	2 412	1 262
березень	5 651	1 974	2 411	1 266
квітень	4 917	1 841	1 809	1 266
травень	4 723	1 765	1 692	1 266
червень	5 888	2 628	2 022	1 239
липень	6 880	3 438	2 205	1 237

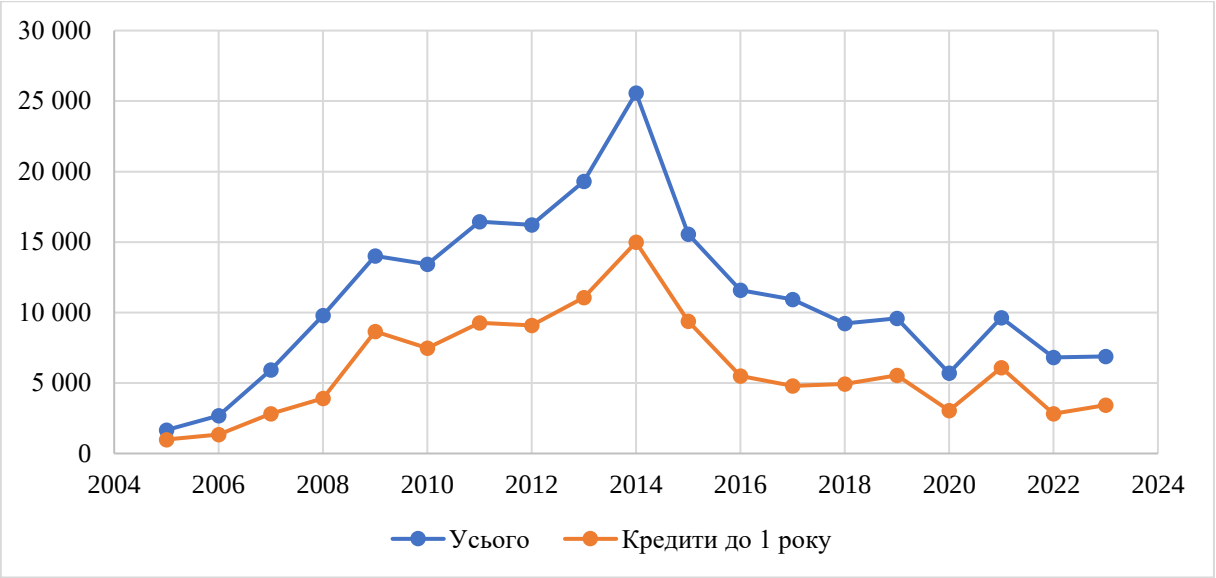


Рисунок 10 – Динаміка наданих кредитів комерційними банками в Україні за 2005–2023 роки

Обсяг наданих кредитів у 2022 та 2023 роках складали 6 809 млн грн (на грудень) та 6 880 млн грн (на липень) відповідно. Ці показники є найменшими за останні десять років. Така ситуація може бути критичною для суб'єктів, які потребують фінансування за рахунок кредитів.

До наступної загрози макроекономічної безпеки було віднесено зменшення трудового потенціалу внаслідок міграції та втрат населення через бойові дії.

За даними Управління Верховного комісара ООН у справах біженців (УВКБ ООН), станом на 26 червня 2023 року в Європі перебуває 5 млн 977 тис. українських переселенців. За межами Європи перебуває ще майже 362 тис. осіб. Водночас, за даними УВКБ ООН, найбільше українців перебуває в Німеччині (1,07 млн осіб), Польщі (994 тис. осіб), Чехії (345 тис. осіб).

Така інформація сформована на основі опублікованої або отриманої від органів влади понад 40 країн інформації про кількість українських переселенців у їхніх державах (у тому числі в Росії та Білорусі).

Нагадаємо, що Управління Верховного комісара ООН у справах біженців (УВКБ ООН) є провідною організацією, що займається захистом прав і добробуту біженців, шукачів тимчасового притулку та осіб без громадянства по всьому світу. Способом реалізації мандату цієї організації є збір, аналіз і розповсюдження даних про становище відповідних груп населення *(Ukrinform, 2023)*.

Що стосується сумарної оцінки людських втрат внаслідок російського вторгнення Україну, маємо зазначити таке: у серпні 2023 року було опубліковано дані New York Times,

згідно з якими число жертв у військах України й Росії сягнуло 500 тис. осіб: Україна втратила 70 тис. загиблими і 100-120 тис. пораненими, Росія втратила 120 тис. загиблими і 170-180 тис. пораненими.

Взагалі необхідно зазначити, що демографічна ситуація – один із найскладніших викликів, з якими стикнулася Україна з часу відновлення незалежності в 1991 році.

У 1990 році в статистичних збірниках зазначалося, що кількість українців складає 52 млн осіб. Але переважання смертності над народжуваністю, масова еміграція населення, зокрема молоді, низький коефіцієнт народжуваності та складна соціально-економічна ситуація зробили депопуляцію характерним для України явищем.

На сьогоднішній момент інформації, скільки людей проживало в Україні до повномасштабного вторгнення, немає.

Так, за оцінками уряду, в Україні (без тимчасово окупованих територій) станом на 1 грудня 2019 року проживало 37,3 млн осіб. Натомість Державний комітет статистики станом на 1 лютого 2022 року оцінював кількість наявного населення (без урахування тимчасово окупованої АР Крим) у 41,1 млн осіб. Річне скорочення статистичні дані показували на рівні понад 420 тис. осіб.

За оцінкою Євростату, станом на 1 січня 2022 року, населення України становило 41 млн осіб. Згідно з оцінкою Світового банку, у 2021 році в Україні проживало 43,8 млн осіб. Орієнтовно такі самі дані наводила ООН.

Тобто навіть за найскромнішими підрахунками, населення України за 30 років скоротилося на понад 8 млн осіб *(Wikipedia, 2024)*.

На жаль, повномасштабне російське вторгнення прискорило депопуляцію та спричинило справжню демографічну катастрофу (десятки тисяч загиблих та поранених, мільйони внутрішньо переміщених осіб та емігрантів). Вищенаведені дані показують значне зменшення трудового потенціалу в країні.

Наступною загрозою економічної безпеки України є зростання індексу споживчих цін (інфляції) *(Minfin, 2023)*.

У табл. 4 наведено індекс інфляції в Україні за 2000–2023 роки.

Таблиця 4 – Індекс інфляції в Україні за 2000–2023 роки, %

Роки	Інфляція за рік	Роки	Інфляція за рік
2000	125,8	2012	105,0
2001	106,1	2013	100,5
2002	99,4	2014	124,9
2003	108,2	2015	143,3

2004	112,3	2016	112,4
2005	110,3	2017	113,7
2006	111,6	2018	109,8
2007	116,6	2019	104,1
2008	122,3	2020	105,0
2009	112,3	2021	110,0
2010	109,1	2022	126,6
2011	104,6	2023	102,5

Нагадаємо, що індекс споживчих цін виявляє зміну вартості фіксованого споживчого набору товарів та послуг у поточному періоді відносно попереднього. Споживчий набір товарів та послуг – це набір найбільш уживаних і важливих для споживання в домогосподарствах товарів та послуг. Встановлюється централізовано і є єдиним для всіх регіонів України.

Проаналізований показник індексу споживчих цін, як й інші макроекономічні показники, демонструє, що як тільки ситуація в Україні починала стабілізуватися, у країні відбувалися кризи, які були пов'язані (в основному) з агресивними діями РФ проти України. Отже, можемо дійти висновку, що ще однією причиною сучасної війни є дестабілізація економічного стану України.

Для характеристики показника приватного споживання проаналізуємо показник реальної заробітної плати в Україні за 2010–2022 роки (табл. 5).

Таблиця 5 – Заробітна плата в Україні за 2010–2022 роки, дол. США

Роки	Середня зарплата	Відхилення до попереднього року		Курс НБУ
		абсолютне, дол.	відносне, %	
за 01.2010	239,5			8,00
за 01.2011	289,3	+49.8	+20.8%	7,94
за 01.2012	340,7	+51.4	+17.8%	7,99
а 01.2013	375,3	+34.6	+10.2%	7,99
за 01.2014	393,8	+18.5	+4.9%	7,99
за 01.2015	213,8	–180.0	–45.7%	16,16
за 01.2016	173,4	–40.4	–18.9%	25,15
за 01.2017	221,5	+48.1	+27.7%	27,12
за 01.2018	275,3	+53.8	+24.3%	28,01
за 01.2019	332,3	+57.0	+20.7%	27,76
за 01.2020	430,5	+98.2	+29.5%	24,92
за 01.2021	437,6	7.1	1.7%	28,19
за 01.2022	506,4	68.9	15.7%	28,78

Середня зарплата в Україні в січні 2022 року склала 14 577 грн, а у 2021 році – 12 337 грн.

За офіційними даними Пенсійного фонду, у березні 2023 року середня зарплата в Україні становила 13 400 тис грн. Якщо взяти за основу курс долара в 36,56 грн/дол., то середня зарплата в дол. США в березні 2023 року складала 365,6 дол. США, тобто порівняно з 2022 роком знизилася на 140,8 дол., або на 27,8%.

Наразі в Україні (у 2023 році) економічно активними є близько 11,7 млн осіб, з яких працюють орієнтовно до 9,3 млн осіб. Ще майже 2,7 млн осіб є безробітними *(Vasylyk S. (ed.), 2023; Minfin, 2024).*

З метою характеристики виробничої безпеки нами було проаналізовано очікування промислових підприємств у січні 2023 року щодо перспектив розвитку їх ділової активності.

У табл. 6 наведено значення індикатору ділової впевненості за 2020–2023 роки

Таблиця 6 – Індикатор ділової впевненості в промисловості за 2020–2023 роки, %

Роки	У промисловості	У переробній промисловості
На 01.2020	-10	-9
На 02.2020	-7	-6
На 03.2020	-6	-5
На 04.2020	-19	-20
На 05.2020	-16	-17
На 06.2020	-14	-14
На 07.2020	-10	-10
На 08.2020	-8	-9
На 09.2020	-9	-10
На 10.2020	-10	-11
На 11.2020	-13	-14
На 12.2020	-15	-19
На 01.2021	-14	-16
На 02.2021	-10	-10
На 03.2021	-6	-6
На 04.2021	-5	-5
На 05.2021	-4	-4
На 06.2021	-5	-5
На 07.2021	-5	-5
На 08.2021	-5	-5
На 09.2021	-4	-6
На 10.2021	-6	-8
На 11.2021	-7	-10
На 12.2021	-10	-14
На 01.2022	-10	-10
На 02.2022	-5	-4
На 03.2022	-25	-26
На 04.2022	-22	-22
На 05.2022	-17	-17
На 06.2022	-16	-16
На 07.2022	-15	-15
На 08.2022	-15	-15

На 09.2022	-14	-14
На 10.2022	-13	-16
На 11.2022	-17	-20
На 12.2022	-19	-21
На 01.2023	-15	-15

У січні 2023 року індикатор ділової впевненості в промисловості підвищився порівняно із груднем 2022 року на 4,2 в. п. і становив мінус 14,9%; у переробній промисловості цей показник підвищився порівняно з попереднім місяцем на 7 в.п. і становив мінус 14,3% *(State Statistics Service of Ukraine, 2023).*

На основі даних табл. 6 побудовано графік динаміки індикатору ділової впевненості в Україні за 2020–2023 роки.

Також показником, який опосередковано показує рівень виробничої безпеки є оцінка поточного обсягу замовлень на виробництво продукції (попиту) в промисловості. У табл. 7 наведено показник оцінки попиту на продукцію промисловості в Україні.

Таблиця 7 – Індикатор поточного обсягу замовлень на виробництво продукції (попиту) у промисловості за 2020–2023 роки, %

Роки	У промисловості	У переробній промисловості
На 01.2020	-42	-44
На 02.2020	-40	-42
На 03.2020	-43	-44
На 04.2020	-46	-50
На 05.2020	-50	-55
На 06.2020	-50	-54
На 07.2020	-46	-51
На 08.2020	-45	-50
На 09.2020	-46	-49
На 10.2020	-44	-45
На 11.2020	-41	-45
На 12.2020	-41	-45
На 01.2021	-40	-45
На 02.2021	-41	-45
На 03.2021	-40	-44
На 04.2021	-34	-36
На 05.2021	-30	-35
На 06.2021	-31	-35
На 07.2021	-32	-36
На 08.2021	-31	-35
На 09.2021	-32	-37
На 10.2021	-32	-37
На 11.2021	-31	-36
На 12.2021	-30	-35

На 01.2022	-30	-33
На 02.2022	-30	-33
На 03.2022	-56	-63
На 04.2022	-55	-60
На 05.2022	-55	-56
На 06.2022	-54	-55
На 07.2022	-54	-55
На 08.2022	-55	-56
На 09.2022	-52	-55
На 10.2022	-51	-54
На 11.2022	-53	-55
На 12.2022	-53	-55
На 01.2023	-53	-55

Дані табл. 7 демонструють, що оцінка поточного обсягу замовлень на виробництво продукції (попиту) в промисловості у 2023 році становила мінус 53%, у переробній промисловості – мінус 55%.

Наведені дані демонструють, що розпочата РФ війна проти України суттєво погіршила як ділову активність, так і попит у промисловості.

Можемо зазначити, що агресія РФ мала на меті економічне погіршення виробничого потенціалу України.

Окремою складовою економічної безпеки є фінансова безпека. Війна суттєво вплинула і на рівень дефіциту державного бюджету.

У табл. 8 наведено доходи та видатки зведеного бюджету України за 2022–2023 роки *(Minfin, 2024)*.

Нагадаємо, що Зведений бюджет України – це сукупність усіх бюджетів, що входять до складу бюджетної системи України. Зведений бюджет України включає Державний бюджет України, бюджет АР Крим та місцеві бюджети. Найважливіше місце в системі державних фінансів належить Державному бюджету.

На основі показників табл. 8 побудовано графік дефіциту Зведеного бюджету України за 2022–2023 роки.

У табл. 8 та на рис. 11 значення показників по місяцях (доходи, видатки, кредитування) надаються в напрямку зростання.

Таблиця 8 – Доходи та видатки Зведеного бюджету України за 2022–2023 роки, млн грн

Роки	Доходи	Видатки	Кредитування	Сальдо (профіцит, дефіцит бюджету)
1	2	3	4	5
Січень 2022	117137,4	83707,7	2755,1	30674,6

Лютий 2022	271269,0	221192,7	1613,7	48370,7
Березень 2022	418465,8	447336,9	2440,4	-31311,5
Квітень 2022	527895,0	641875,0	1694,1	-115673,6
Травень 2022	669315,8	884013,9	254,5	-214962,5
Червень 2022	809170,9	1157712,0	333,7	-349031,4
Липень 2022	1022509,4	1366385,5	413,7	-344289,8

Продовження таблиці 8

1	2	3	4	5
Серпень 2022	1283822,8	1620715,5	206,7	-337099,4
Вересень 2022	1537743,0	1944418,4	732,8	-407408,2
Жовтень 2022	1660641,3	2208877,8	-1721,3	-546517,7
Листопад 2022	1840177,6	2555396,2	-3090,9	-712131,7
Грудень 2022	2196273,3	3043499,1	-2397,9	-844827,9
Січень 2023	154515,7	204976,0	-268,7	-50191,6
Лютий 2023	351737,2	481822,7	-1030,2	-129055,2
Березень 2023	627644,0	809469,7	-1313,0	-180512,7
Квітень 2023	925539,6	1128878,9	-2534,9	-200804,4
Травень 2023	1238812,1	1524718,8	-5529,0	-200804,4
Червень 2023	1518574,1	1937572,1	-5361,1	-413637,0
Липень 2023	1733223,4	2243134,8	-5472,4	-504439,0

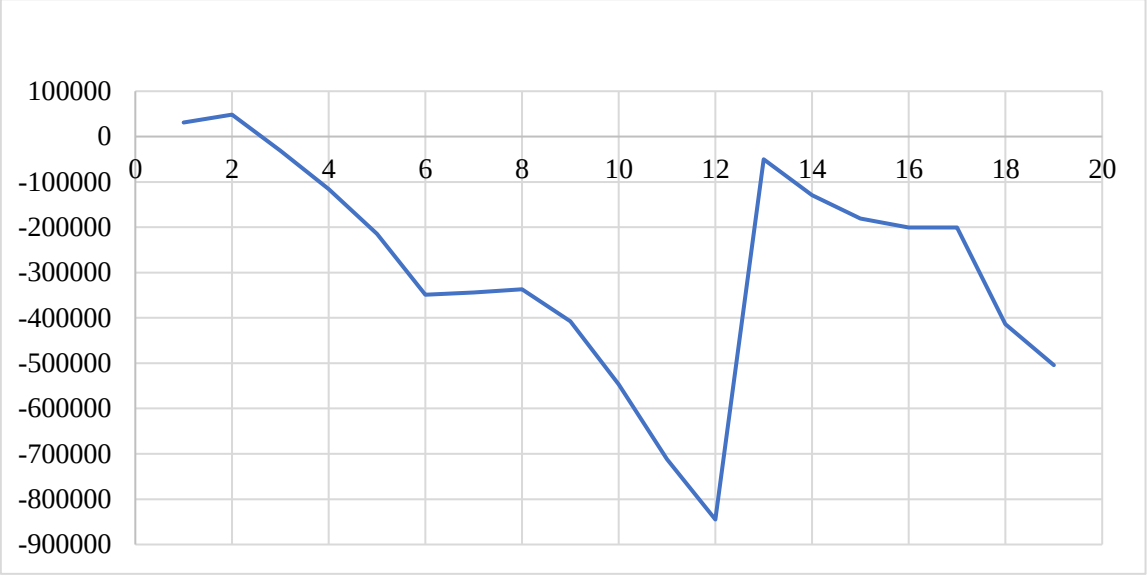


Рисунок 11 – Дефіцит зведеного бюджету України за 2022–2023 роки

У табл. 9 наведено показники зведеного бюджету України в динаміці за 2011–2022 роки.

За даними табл. 9 спостерігаємо, що дефіцит зведеного бюджету України складав більше 16% ВВП, що є найгіршим показником з 2011 року *(State Statistics Service of Ukraine, 2023; Minfin, 2024).*

На основі даних, наведених у табл. 9 побудовано графік розміру дефіциту зведеного бюджету до ВВП.

Таблиця 9 – Показники зведеного бюджету України в динаміці за 2011–2022 роки, млн грн

Роки	Доходи		Видатки		Кредитування		Сальдо (дефіцит бюджету)	
	млн грн	% ВВП	млн грн	% ВВП	млн грн	% ВВП	млн грн	% ВВП
2011	398553,6	30.27	416853,6	31.66	4757,9	0.36	-23057,9	-1.75
2012	445525,3	31.62	492454,7	34.95	3856,3	0.27	-50785,7	-3.60
2013	442788,7	30.43	505843,8	34.77	535,2	0.04	-63590,3	-4.37
2014	456067,3	29.11	523125,7	33.39	4972,1	0.32	-72030,5	-4.60
2015	652031,0	32.94	679871,4	34.35	3057,8	0.15	-30898,2	-1.56
2016	782748,5	32.84	835589,8	35.06	1841,3	0.08	-54682,6	-2.29
2017	1016788,3	34.09	1056759,9	35.43	2122,1	0.07	-42093,8	-1.41
2018	1184278,1	33.28	1250173,6	35.13	1893,0	0.05	-67788,5	-1.90
2019	1289779,8	32.45	1370113,0	34.47	3983,2	0.10	-84316,4	-2.12
2020	1376661,6	32.82	1595289,7	38.04	5316,2	0.13	-223944,3	-5.34
2021	1662242,7	30.45	1844377,7	33.78	4773,2	0.09	-186908,3	-3.42
2022	2196273,3	42.31	3043499,1	58.63	-2397,9	-0.05	-844827,9	-16.27

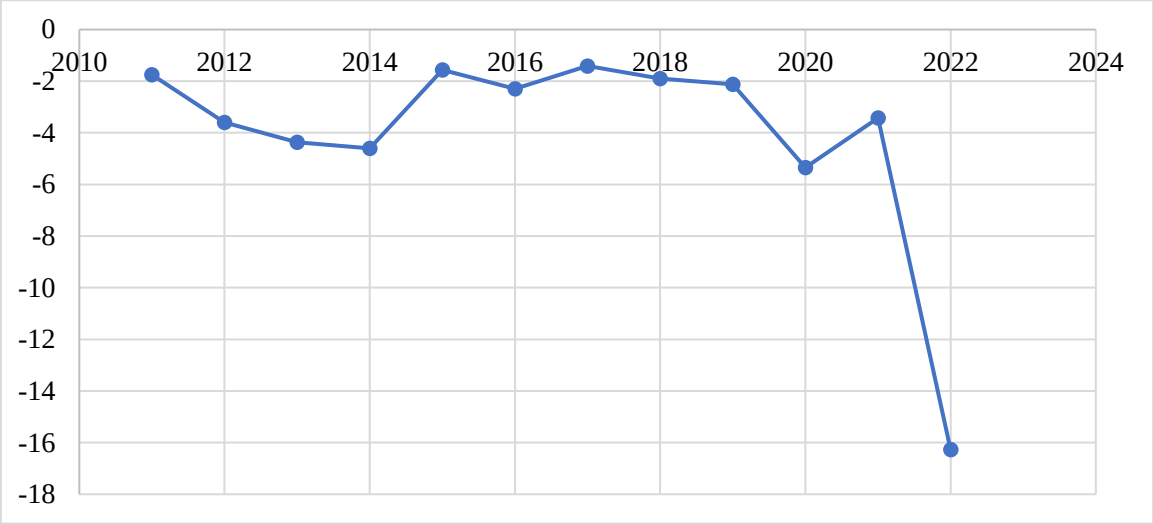


Рисунок 12 – Динаміка дефіциту Зведеного бюджету України до ВВП

Наступним показником, який характеризує фінансову безпеку, є державний борг.

Нагадаємо, що державний борг є сукупністю боргових зобов'язань держави перед усіма кредиторами (юридичними та фізичними особами, іноземними державами, міжнародними організаціями тощо). Державний борг складається із заборгованості центрального уряду,

регіональних та місцевих органів влади, а також боргів усіх корпорацій з державною участю, пропорційно частці держави в їх капіталі.

Державний борг традиційно поділяють на зовнішній та внутрішній.

Зовнішній державний борг – це заборгованість держави іншим країнам, міжнародним економічним організаціям та іншим особам. Державний зовнішній борг є частиною валового зовнішнього боргу країни.

Внутрішній державний борг – це заборгованість держави власникам державних цінних паперів та іншим кредиторам.

Власне державний борг виникає внаслідок фінансових запозичень держави, договорів й угод про надання кредитів та позик, пролонгації та реструктуризації боргових зобов'язань минулих років. Сукупність боргових зобов'язань держави містить також гарантований державою борг, що виникає в наслідок прийнятих на себе державою гарантій за зобов'язаннями третіх осіб, або прийняті на себе державою зобов'язання третіх осіб.

У табл. 10 наведено структуру державного та гарантованого державою боргу за даними Міністерства фінансів України на 31.07.2023 року.

Таблиця 10 – Структура державного та гарантованого державою боргу на 31 липня 2023 року, млн грн

Борг	Зовнішній		Внутрішній		Усього	
	млн грн	Питома вага, %	млн грн	Питома вага, %	млн грн	Питома вага, %
Державний борг	3 050 335,1	62,8	1 470 754,2	30,3	4 521 089,3	93,0
Гарантований борг	268 850,0	5,5	70 653,9	1,5	339 503,9	7,0
Сукупний	3 319 185,1	68,3	1 541 408,1	31,7	4 860 593,2	100,0

У табл. 11 наведено інформацію щодо державного та гарантованого державою боргу України, починаючи з 2009 року.

За даними табл. 11 бачимо, що найбільший приріст загального боргу спостерігався у 2014 році (88,4%) та у 2022 році (52,4%). Загальний же борг за період з 2009 року по 2023 рік зріс з 316 884,6 млн грн до 4 860 593,2 млн грн, або в 15 разів.

На рис. 13 наведено інформацію про приріст загального державного боргу України за 2009–2023 роки.

За даними табл. 11 та рис. 13 бачимо, що з 2009 року загальний приріст загального державного боргу склав більше ніж 300%.

Таблиця 11 – Державний та гарантований державою борг України в динаміці за 2009–2023 роки, млн грн

Роки	Загальний борг		Зовнішній борг	Внутрішній борг
	млн грн	Приріст до попереднього року, %		
на 31.12.2009	316 884,6		211 751,7	105 132,9
на 31.12.2010	432 235,4	36,4	276 745,6	155 489,8
на 31.12.2011	473 121,6	9,5	299 413,9	173 707,7
на 31.12.2012	515 510,6	9,0	308 999,8	206 510,7
на 31.12.2013	584 114,1	13,3	300 025,4	284 088,7
на 31.12.2014	1 100 564,0	88,4	611 697,1	488 866,9
на 31.12.2015	1 572 180,2	42,9	1 042 719,6	529 460,6
на 31.12.2016	1 929 758,7	22,7	1 240 028,7	689 730,0
на 31.12.2017	2 141 674,4	11,0	1 374 995,5	766 678,9
на 31.12.2018	2 168 627,1	1,3	1 397 217,8	771 409,3
на 31.12.2019	1 998 275,4	-7,9	1 159 221,6	839 053,8
на 31.12.2020	2 551 935,6	27,7	1 518 934,8	1 033 000,8
на 31.12.2021	2 671 827,6	4,7	1 560 230,0	1 111 597,6
на 31.12.2022	4 071 683,1	52,4	2 610 945,6	1 460 737,5
на 31.12.2023	4 860 593,2	19,.4	3 319 185,1	1 541 408,1

У табл. 12 наведено дані Інституту світової економіки Кіля (Kiel Institute for the World Economy), які включають оцінку військової, фінансової та гуманітарної допомоги, переданої урядами різних країн Україні.

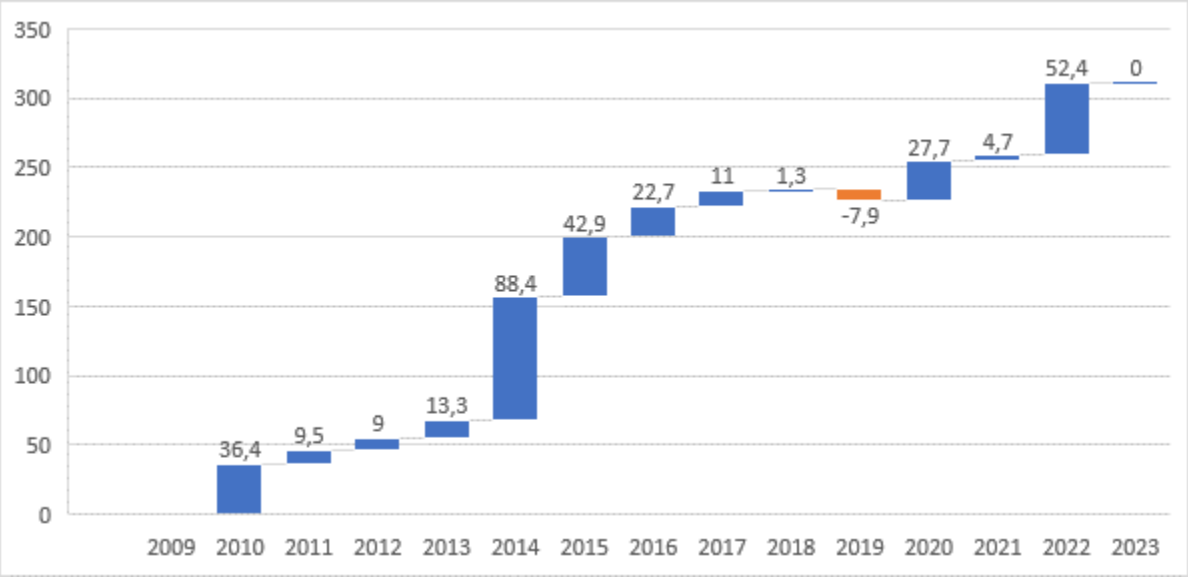


Рисунок 13 – Приріст загального державного боргу України за 2009–2023 роки

Військова допомога включає всі види озброєння та військової техніки, а також предмети, передані українській армії, та фінансову допомогу на військові цілі. Гуманітарна допомога – це підтримка цивільного населення (в основному продовольство, медикаменти та інші предмети допомоги). Фінансова допомога включає гранти, позики, гарантії та своп-лінії.

Закон про ленд-ліз для України підписано президентом США Д. Байденом 9 травня 2022 року. Механізм ленд-лізу з 1941 року ні одного разу не запускався для жодної з країн у світі попри всі війни. які відбувалися.

Ленд-ліз для України показує безпрецедентну важливість цього акту з боку США. Згідно закону про ленд-ліз, Україна отримуватиме стільки допомоги, скільки необхідно для перемоги, і такою зброєю буде будь-яка зброя, окрім зброї масового ураження та її комплектування. Рішення про передачу озброєння прийматиметься за прискореною процедурою. Згідно із вищезазначеним законом, президент США просто уповноважує уряд надавати допомогу в тому розмірі, який необхідний.

Передача озброєння буде результатом запитів України та реальних можливостей США, які спираються на доволі потужні арсенали із тисячами одиницями бронетехніки, а також нарощування можливостей власного оборонно-промислового комплексу.

Таблиця 12 – Оцінка військової, фінансової та гуманітарної допомоги (зобов'язання), переданої урядами різних країн Україні на 20 листопада 2022 року, млн євро

Країна	Фінансова	Гуманітарна	Військова	Разом
1	2	3	4	5
Австралія	–	51,4	269,1	320,4
Австрія	10,0	566,5	3,6	580,1
Бельгія	5,0	117,2	96,0	218,2
Болгарія	–	0,7	3,8	4,5
Велика Британія	2554,9	397,8	4129,2	7081,8
Греція	–	–	191,2	191,2
Данія	57,5	73,6	510,0	641,1
Естонія	–	5,0	330,0	335,0
ЄС (Рада Європи та комісії)	28320,0	1570,0	–	29890,0
Індія	–	1,9	–	1,9
Ірландія	–	68,7	–	68,7
Іспанія	200,0	101,0	81,1	382,1
Італія	310,0	43,4	319,1	672,5
Канада	2139,1	287,8	1356,7	3783,6
Китай	–	2,1	–	2,1
Кіпр	–	2,5	–	2,5
Латвія	15,0	1,4	297,1	313,5
Литва	5,0	57,0	198,7	260,7
Люксембург	–	4,0	72,0	76,0
Мальта	–	1,2	–	1,2
Нова Зеландія	–	2,3	14,7	17,0
Норвегія	324,2	325,6	560,1	1209,9
Нідерланди	348,5	208,9	289,8	847,2
Німеччина	1150,0	1950,0	2344,9	5444,9
Польща	1002,9	175,3	1822,4	3000,6
Португалія	250,0	1,2	83,6	334,8

Південна Корея	–	90,9	3,6	94,4
Румунія	–	7,8	3,0	10,8
США	15053,3	9903,9	22862,0	47819,2
Словаччина	–	5,0	210,2	215,2
Словенія	–	2,1	58,8	60,9
Тайвань	–	68,3	–	68,3
Туреччина	–	0,2	64,2	64,4
Угорщина	–	46,7	–	46,7
Франція	800,0	142,5	471,7	1414,2
Фінляндія	81,5	46,2	177,9	305,6
Хорватія	–	6,4	16,5	22,9
Чехія	–	108,2	478,5	586,7
Швейцарія	–	202,8	–	202,8
Швеція	152,5	107,8	546,2	806,5
Японія	597,9	5,6	2,4	606,0
Усього	53377,2	16760,9	37868,0	108006,0

Механізм ленд-лізу передбачає передачу не лише зброї, а й усього іншого, що необхідно для перемоги України. Це передача ресурсів, компонентів або взагалі цивільної техніки.

Допомога США для України у формі ленд-лізу визначена на рівні 20,4 млрд. дол. США і буде спрямована виключно на військовий та безпековий сегмент для України

Назва «Lend-Lease» перекладається з англійської мови як «позика-оренда». Можемо натрапити на варіанти тлумачення цього поняття як про таке, що ця допомога для України буде безоплатною. Насправді ж у законі про ленд-ліз щодо оплати зазначено лише про скасування загальної вимоги оплати на передану допомогу протягом п'яти років. Обсяг у 20,4 млрд. дол. США дорівнює понад 20 річних бюджетів Міноборони України на закупівлю й модернізацію всієї техніки та зброї, тобто за масштабами це є дійсно значною допомогою. Україна згодом цілком може її оплатити, зокрема, як варіант, правом розміщення військових баз, наприклад, у Севастополі *(Defense Express, 2022)*.

З перших тижнів російського вторгнення стало очевидним, що РФ цілеспрямовано руйнує українські міста та інфраструктуру. Відновлення вимагатиме після закінчення війни величезних ресурсів.

У контексті повоєнного розвитку України спеціалісти розглядають певну фінансову супердопомогу, котра має забезпечити стрімке відновлення економіки нашої держави подібно до відродження країн Західної Європи, які були реципієнтами плану Маршалла в 1948–1951 роках.

Оскільки саме план Маршалла став синонімом програм післявоєнної відбудови, уже на початку квітня 2022 року ця ідея обговорювалася у МВФ та Світовому банку саме під цим знаковим для європейської історії визначенням для України.

І хоча оригінальний план Маршалла запрацював лише через три роки після завершення Другої світової війни, для України світове співтовариство готове діяти на випередження.

Перший найбільш деталізований варіант такої програми (A Blueprint for the Reconstruction of Ukraine) наприкінці квітня 2022 року запропонували в британському Центрі досліджень економічної політики (CEPR). До його розробки долучилися кілька експертів Стокгольмської школи економіки, Гарвардського університету, Каліфорнійського університету в Берклі та Массачусетського технологічного університету. Від України до експертного пулу увійшла команда на чолі з радником голови Адміністрації президента України Т. Мілововим.

За версією розробників, ключове адміністрування плану Маршалла має покладатися на недержавне агентство з інвестицій та відновлення з широкою автономією в оперативному управлінні проектами, при тому, що «власником» програми реконструкції залишатиметься Україна. Обсяг допомоги становитиме 500 млрд. дол. США, але з урахуванням остаточних збитків на момент завершення гарячої фази бойових дій.

Українській уряд та міжнародна експертна команда оцінила втілення плану Маршалла для України в 765 млрд. дол. США терміном до 2032 року. З них 65 млрд. дол. США має бути залучено вже у 2023 році й близько 300 млрд. дол. США – на етапі так званого Fastrecovery (швидкого відновлення) у 2023–2026 роках з фокусом на соціальну інфраструктуру та інженерні комунікації.

План також повинен врахувати стратегічні інтереси країн-донорів. Зокрема, компанії з ЄС матимуть пріоритетне право на контракти у сфері інфраструктури, житлового будівництва, транспорту тощо, у тому числі з урахуванням міграції сучасних технологій в Україну.

Наступна частина плану – Modernisation (модернізація) у 2026–2032 роках – це близько 400 млрд. дол. США. Ця частина включатиме максимізацію в українській економіці продукції з високою доданою вартістю та мінімізацію «карбонового сліду».

Уже на 2023 рік передбачені інвестиції в розмінування 5% території країни, підготовку енергосистеми до зимового періоду та накопичення газу, страхування інвестицій від воєнних ризиків, початок будівництва вантажного коридору до м. Клайпеди через Польщу, ремонту 20 000 пошкоджених війною будинків та будівництво 100 000 нових житлових споруд.

Подальший план інвестицій передбачає появу в Україні впродовж наступних 10 років залізничної інфраструктури європейського стандарту, нових блоків АЕС та орієнтованих на європейський ринок індустріальних кластерів.

Структурно українська візія плану Маршалла розподілена на 15 сегментів. До нього також включено понад 50 млрд. дол. США на обороноздатність країни та перезапуск ОПК з урахуванням стандартів NATO. Технічно це відбуватиметься через Оборонну технологічну

агенцію (аналог американської DARPA) та Оборонний акселератор DiiaTechand Defense (за зразком Diia City), в екосистемі якого сьогодні в Україні працює більшість IT-спеціалістів.

За словами колишнього міністра оборони України О. Резнікова, Україна у 2023 році уже стала асоційованим членом програми технологічного співробітництва збройних сил країн NATO, відповідно має право розробляти та вносити зміни до ключових стандартів NATO.

Пріоритетним джерелом надходження коштів за планом Маршалла мають стати заморожені активи країни-агресора та олігархів з найближчого оточення президента РФ.

Також передбачено отримання коштів від міжнародних донорів. За даними агентства Bloomberg, лише у Єврокомісії планують виділити на відновлення України 523 млрд. дол. США

Україна зі свого боку в інтересах прозорості використання коштів має провести цифровізацію державних реєстрів та забезпечити обмежений доступ до них.

Мірилом успішної реалізації українського плану Маршалла є щонайменш 7% зростання економіки щороку, а також входження України до переліку 25 провідних країн за Індексом людського капіталу, де 2020 році Україна посідала лише 53 позицію *(Rybakov D., 2022)*.

Негативна трансформація вітчизняного виробництва під час війни супроводжується однією із суттєвих загроз економічній безпеці на сучасному етапі, а саме – соціальною.

Висновки. У кожній країні наявна своя специфіка та стратегія розвитку напрямів економічної безпеки, у тому числі з урахуванням процесу глобалізації. Так, з метою забезпечення економічної безпеки країни, Україні необхідно визначити пріоритети її соціально-економічного розвитку, соціальної політики на основі виявлення тенденцій економічної політики. Також слід визначити шляхи підвищення ефективності реалізації соціальних стратегій з метою збільшення доходів бюджету, підтримки достатнього рівня виробничого, науково-технічного потенціалу, недопущення зниження рівня життя населення.

Водночас слід зазначити, що без урахування закономірностей функціонування глобальної економічної системи, тенденцій її розвитку та факторів диференціації окремих економік за рівнем розвитку в її межах усі розробки з економічної безпеки України будуть малоефективними.

Отже, варто наголосити, що визначення порогового значення економічної безпеки країни в умовах глобалізації та забезпечення її економічної безпеки є вельми актуальними.

На сьогодні разом зі збереженням високого рівня зовнішньої загрози з'явилася тенденція наростання загроз, що мають внутрішню природу походження.

На жаль, Україна сьогодні є слабким учасником міжнародної конкуренції, на нашу думку, саме загострення конкуренції, що викликане глобалізацією, і є однією з причин

сучасної війни. Аналіз основних показників економічної безпеки показав, що РФ протягом останніх десяти років не допускала стабілізації та економічного зростання в Україні, у будь-який спосіб створюючи кризи (спочатку у 2014, а потім – у 2022 роках).

References:

Геоекономіка. URL: https://ru.wikipedia.org/wiki/Геоэкономика.

Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

Концепція зовнішньої політики України. 2020. URL: http://fes.kiev.ua/n/cms/fileadmin/upload2/Koncepcija_zovnishnoji_politiki_Ukrajini_05.10_1.pdf

Актуальні виклики та загрози економічній безпеці України в умовах воєнного стану. Національний інститут стратегічних досліджень. 2023. URL: https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/aktualni-vyklyky-ta-zahrozy-ekonomichniy-bezpetsi-ukrayiny-v

Валовий внутрішній продукт (ВВП) в Україні. URL: https://index.minfin.com.ua/ua/economy/gdp/

Прямі іноземні інвестиції (ПІІ) в Україну. URL: https://index.minfin.com.ua/ua/economy/fdi/

Статистика фінансового сектору. НБУ. URL: https://bank.gov.ua/ua/statistic/sector-financial

Кількість українців та їх міграція за кордон через війну. Укрінформ. 2023. URL: https://www.ukrinform.ua/rubric-ato/3732355-kilkist-ukrainciv-ta-ih-migracia-za-kordon-cerez-vijnu.html

Втрати у російсько-українській війні (з 2014). URL: https://cutt.ly/fwE0pixL

Індекс інфляції в Україні 2023. URL: https://index.minfin.com.ua/ua/economy/index/inflation/

Тенденція зберігається. Стало відомо, на скільки зросла середня зарплата в Україні. URL: https://biz.nv.ua/ukr/economics/zarplata-2023-na-skilki-zrosla-serednya-zarplata-v-ukrajini-50336985.html

Середня зарплата в Україні. URL: https://index.minfin.com.ua/ua/labour/salary/average/

Стан ділової активності промислових підприємств. URL: https://www.ukrstat.gov.ua/operativ/operativ2023/fin/rp/prom/prom_01_2023_u.pdf

Зведений бюджет України. URL: https://index.minfin.com.ua/ua/finance/budget/cons/2022/

Підтримка України у світі. URL: https://index. minfin.com.ua/ua/russian-invading/supporting-ukraine/

Ленд-ліз для України підписано: яку зброю отримаємо та коли оплачувати. 2022. URL: https://defence-ua.com/minds_and_ideas/lend_liz_dlja_ukrajini_pidpisano_jaku_zbroju_otrimajemo_ta_koli_oplachuvati-7294.html

Рибаков Д. (2022). Відновити все: що варто знати про «План Маршалла» для України та його історичні витоки. 2022. URL: https://mind.ua/publications/20244464-vidnoviti-vse-shcho-varto-znati-pro-plan-marshalla-dlya-ukrayini

Іванов С. В. (2023). Приводи й причини війни РФ проти України: економічний контекст : монографія. Дніпро: Журфонд, 2023. 184 с.

Іванов С. В., Разумова Г. В. (2023). Продовольча безпека України в умовах війни і повоєнної відбудови. Відбудова для розвитку: зарубіжний досвід та українські перспективи : міжнародна колективна монографія / [редколегія, голова – д.е.н. В.В.Небрат] ; НАН України, ДУ «Ін-т екон. та прогнозув. НАН України». Київ, 2023. С. 441-454.

Разумова Г. В., Оскома О.В. (2023). Шляхи вдосконалення кредитної політики НБУ в умовах воєнного стану. Проблеми сучасних трансформацій. Серія: економіка та управління. 2023. № 9. https://doi.org/10.54929/2786-5738-2023-9-08-07.

Іванов С. В. (2023). Продовольча безпека України в умовах сучасних викликів: монографія. НАН України, ДУ «Ін-т. ринку і екон.-екол. дослідж. НАН України». Одеса : ДУ «ІРЕЕД НАНУ», 2023. 291 с.

DOI 10.5281/zenodo.10820567
UDC 334.78:005.35]:004.9.056

CHAPTER 8.
ORGANIZATIONAL AND ECONOMIC MECHANISM OF CORPORATE MANAGEMENT OF ENTERPRISES IN THE FIELD OF CYBER SECURITY IN CONDITIONS OF ECONOMIC UNCERTAINTY

Iryna KALINA
Dr.Sc. (Econ), . Ph.D., Professor of Marketing
Educational and scientific institute of economic and business management,
Interregional Academy of Personnel Management,
Kyiv, Ukraine
2 Frometivska Street, Kyiv, Ukraine
kalinargz@gmail.com,
https://orcid.org/0000-0001-5662-6967

Abstract. The topic is dedicated to the solution of an important scientific and applied problem related to the justification and development of theoretical and methodological principles and scientific and practical recommendations for the development of corporate management of enterprises in the field of cyber security. The conceptual and categorical apparatus of such terms as "corporation", "corporate management", which have been transformed taking into account information and communication technologies, has been studied. The organizational and economic mechanism of corporate management of enterprises in the field of cyber security has been improved, which combines three blocks: regulatory and legal support, organizational and economic support, informational and management support. This in aggregate ensures the peculiarities of the creation and functioning of the mechanism, in the individuality and integral unity of such elements, as well as in the achievement of the outlined economic and social results.

Keywords: corporate governance, mechanism, development, cyber security, conditions, economic uncertainty, information, components of the corporate governance mechanism, cyber security enterprises, strategy.

ОРГАНІЗАЦІЙНО-ЕКОНОМІЧНИЙ МЕХАНІЗМ КОРПОРАТИВНОГО УПРАВЛІННЯ ПІДПРИЄМСТВ У СФЕРІ КІБЕРБЕЗПЕКИ В УМОВАХ ЕКОНОМІЧНОЇ НЕВИЗНАЧЕНОСТІ

Анотація. Тема присвячена вирішенню важливої науково-прикладної проблеми, пов'язаної з обґрунтуванням і розробкою теоретико-методичних засад та науково-практичних рекомендацій щодо розвитку корпоративного управління підприємств у сфері кібербезпеки. Досліджено понятійно-категоріальний апарат таких термінів як «корпорація», «корпоративне управління», які трансформовані із врахуванням інформаційно-комунікаційних технологій. Вдосконалено організаційно-економічний механізм корпоративного управління підприємств у сфері кібербезпеки, який поєднує три блоки: нормативно-правове забезпечення, організаційно-економічне забезпечення, інформаційно-управлінське забезпечення. Це в сукупності забезпечує особливості створення й функціонування механізму, в індивідуальності й інтегральній єдності таких елементів, а також у досягненні накреслених економічних і соціальних результатів.

Ключові слова: корпоративне управління, механізм, розвиток, кібербезпека, умови, економічна невизначеність, інформація, складові механізму корпоративного управління, підприємства сфери кібербезпеки, стратегія.

Вступ. На сучасному етапі розвитку інформаційно-комунікаційних відносин в Україні надзвичайної актуальності набувають проблеми розробки та впровадження організаційно-економічних механізмів корпоративного управління діяльністю підприємств у сфері кібербезпеки, що реалізували б засади створення високоефективного конкурентоспроможного інформатизаційного сектору України на світовому ринку. Одним з найхарактерніших явищ ринкових трансформацій в Україні стало створення корпоративного сектора економіки як базового серед інших організаційно-правових форм господарювання. Проблематика трансформіції корпоративного управління підприємств у цифровізації залишається актуальними для національної економічному, для всіх підприємств будь якої сфери діяльності у звязку із розширеням локальних можливостей захисту даних, щоб дані завжди були доступні, захищені та активно працювали для розвитку підприємства.

Постановка проблеми. Сучасні тенденції розвитку національної економіки України викликають необхідність по-новому оцінити інформаційні ресурси, що їх використовує підприємство у своїй діяльності, включаючи інформаційну безпеку. Одним з основних напрямків розвитку України з моменту впровадження цифровізаційної ери стали технологічний прогрес та впровадження інформаційних технологій, які сьогодні суттєво

полегшують процеси пошуку та оперування інформацією. Але з цифровізаційним впровадженням і посилилас небезпека, щодо викрадання інформації як підприємств так і персональних даних співробітників та клієнтів, а також виведення зладу роботи підприємства, якщо використовувати різноманітні кібератаки. Розвиток корпоративного управління підприємств через низку спектрів галузевих проблем залишається важливою складовою структурного реформування, що зумовило актуалізацію наукових досліджень різнопланового інформаційно-економічного змісту. Питання полягає у досягненні економічної ефективності за умов реалізації різних цілей корпоративного управління, а саме підвищення ефективності функціонування підприємств і забезпечення балансу інтересів зацікавлених сторін. Як показав аналіз, досягнення цих двох цілей є необхідним з точки зору досягнення необхідних темпів економічного зростання, створення та підтримка конкурентного середовища, максимізації прибутковості інвестиційного процесу, підвищення продуктивності праці та ефективності виробництва та надвння послуг. Проблема оцінки якості корпоративного управління об'єктивно ускладнюється різноорієнтованими ціннісними пріоритетами учасників корпоративних відносин. При цьому усі учасники корпоративного управління зацікавлені у досягненні успіху в діяльності підприємства, однак шляхи й методи його забезпечення можуть значно відрізнятися. Саме тому адекватне оцінювання економічної ефективності корпоративного управління дозволяє визначити можливість створення балансу інтересів зацікавлених сторін.

Аналіз останніх досліджень і публікацій. Слід зазначити, що теоретико-методологічні й економіко-організаційні аспекти дослідження корпоративного управління розглянуто в працях таких вітчизняних і зарубіжних вчених, як Воронкова А.Е., Баб'як М. М., Коренєв Е. Н., Мажура І. В. (*Воронкова А.Е., Баб'як М. М., Коренєв Е. Н., Мажура І. В., 2006*), Гриньова В.М., Попов О.Є. (*Гриньова В.М., Попов О.Є., 2003*), Краковський О. (*Краковський О., 2000*), Дмитренко М. Й. (*Дмитренко М. Й., 2014*), Пономаренко В.С., Ястремська Є.М., Луцьківський В.М. , Кушнар С.Л., Ріпка Д.А., Бєлікова Н.В. (*Пономаренко В.С. та інші, 2006*)

Вчені, які приділили увагу безпосередньо новому поняттю «кібербезпека» та її вплив на розвиток підприємства під дією різних факторів (економічний, соціальний, юридичний, інноваційний тощо) це: Арістова І.В., Сулацький Д. В. (*Арістова В. І., Сулацький Д. В., 2013*) Арсенович Л.А., (*Арсенович Л.А., 2021*), Кириченко Л., Радівілова Т.А., Карлссон А. (*Кириченко Л., Радівілова Т.А., Карлссон А., 2018*).

Аналіз наукових доробків показав, що тематика є ще недостатньо дослідженою як у теоретичному, так і в практичному аспектах, адже цифровізація розвивається та кожного дня з'являються нові методи, принципи та закони кібербезпеки.

1. Дефініція поняття корпоративне управління в нових реаліях ведення бізнесу.

У зв'язку з розвитком підприємницької діяльності та різних форм власності та організації виробництва в Україні актуалізується значення категорії «корпорація» та «корпоративне управління». Корпорація історично виникла в результаті еволюції ринкових відносин як економічний інститут об'єднання капіталу для фінансування великих підприємницьких проектів, що забезпечило їй широку перспективу. У вітчизняній економіці ця форма господарства була використана головним чином як засіб ринкової трансформації економіки в процесі управління формами власності великих підприємств, внаслідок чого вона стала інструментом перерозподілу прав власності та активів держави. За умов поглиблення загальної соціально-економічної кризи в Україні це призвело до занепаду багатьох приватизованих підприємств, інвестиційних обмежень та зростаючого соціального невдоволення масовою приватизацією. Отже, на етапі зародження корпорацій науковий і практичний інтерес являє собою вивчення досвіду корпоративного господарювання, уточнення його реального потенціалу у ринково-конкурентному середовищі. Слід зазначити, що це поняття не нове і ще А. Сміт у своїй праці «Дослідження про природу та причини багатства народів» застосував категорію «корпорація» в розумінні акціонерної форми організації підприємництва (*Євтушевський В.А., 2002)*. К. Макконнелл, С. Брю та Г.С. Вечканов розкривають корпорацію як «...юридичний суб'єкт (юридична особа), який отримав чартер властей штату чи федерального уряду та відособлений від індивідів, власністю яких він є» (*McConnell K.R., Brew S.L., 1998)*. Отже, корпорація – це юридична особа, окрема та відмінна від своїх власників, що має права, обов'язки і привілеї (*Тарасюк А.В., 2017)*. Американські науковці Р. Тьюлз та Е. Бредлі визначають, що корпорація – підприємницька організація, визнана юридичною особою, яка має обмежену відповідальність і необмежений термін існування та засновується на основі статуту, схваленого комісаром у справах корпорацій штату. Права й обов'язки корпорації регламентуються її статутом та місцевим і федеральним законодавством. Корпорація контролюється акціонерами, що мають право голосу, які обирають директорів, а ті, у свою чергу, призначають інших керівних осіб (*Richard J. Teweles, Edward S. Bradley,1998)*. П. Самуельсон і В. Нордхауз це науковці, які визначають корпорацію як «...юридичну особу, яка може самостійно продавати і купувати, позичати гроші, виготовляти товари й послуги та вступати у контрактні відносини, має право обмеженої відповідальності, у відповідності з яким інвестиції кожного із власників корпорації обмежені жорстко певним розміром» (*Paul Samuelson,William Nordhaus, 2009)*.

Д. Маршал і В. Бансал додають до визначення корпорації те, що вона повністю відокремлена від своїх власників, діє самостійно, а її власники можуть вільно передавати свою

участь у капіталі іншим особам без будь-якого безпосереднього впливу на саму корпорацію (*Marshall, J. and V.K. Bansal, 1992*). І. Ансофф розкриває поняття корпорації так: «Корпорація – це широко поширена в країнах з розвиненою ринковою економікою форма організації підприємницької діяльності, яка передбачає пайову власність, юридичний статус та зосередження функцій управління у руках верхнього ешелону професійних управляючих, працюючих за наймом» (*H. Igor Ansoff., 1988*)

Найбільш повне визначення корпорації надано в Barron's Dictionary of Banking Terms: «Корпорація – ділова організація, розглянута як незалежне утворення – штучна особа, що відрізняється від його власників в очах закону. Власність представлена частками в капіталі. Корпорація має три відмінні характеристики: 1) відділення власності від управління і обмежена відповідальність, тобто її відповідальність перед власниками обмежена її ресурсами, на відміну від товариств або індивідуальних підприємств, де зберігається необмежена відповідальність власників; 2) здатність укладати контракти і володіти власністю; 3) передача права власності, що забезпечує існування корпорації за межами терміну життя її власників. Акціонери обирають корпоративних директорів, які у свою чергу визначають її політику» (*Євтушевський В.А., 2002).*

В цьому визначенні корпорації в найбільшій мірі притаманні риси підприємству – відокремлення власності від управління нею і передача права власності. З метою глибшого дослідження категорії «корпорація» необхідно дослідити її сутність у вітчизняній економіко-правовій системі з врахуванням вітчизняної правової бази. Термін «корпорація» в економічній літературі широко використовується для позначення певним чином організаційних підприємств. Однак цей термін не має однозначного тлумачення. Так, господарським кодекс України визначено, що корпорація – це договірне об'єднання, створене на основі поєднання виробничих, наукових і комерційних інтересів підприємств, що об'єдналися, з делегуванням ними окремих повноважень централізованого регулювання діяльності кожного з учасників органам управління (*Господарський кодекс України, 2022).*

Корпоративне управління, як слідує з визначення поняття «корпорація», це діяльність з метою отримання прибутку для інституційної одиниці. Однак в умовах нової реальності, переходу до цифровізації, на нашу думку, повинна підпорядковуватися не тільки досягненню високого рівня прибутку, але і виконанню певної місії, яка визначається локалізаційними особливостями і функцією інституційної одиниці у суспільстві. Корпоративне управління слід трактувати як управління в нових реаліях, яке здійснюється, по-перше, не тільки через розподіл управлінських функцій між виконавцями, по-друге, через розподіл предметів і результатів діяльності між членами корпорації, по-третє, шляхом інтеграції фінансових

ресурсів і зміни власників (збільшення чи зменшення їх чисельності) через купівлю-продаж акцій корпорацій на фінансовому ринку (*Гриньова В.М., Попов О.Є., 2003*).

При визначенні поняття «корпоративне управління» також існує множина точок зору, які розкривають різні підходи їх авторів до цієї важливої економічної категорії. М. Хессель, який проводить паралель між державним устроєм (виборці – парламент – уряд) та корпоративним управлінням (акціонери – рада директорів – менеджери) (*Dudnyk, O., Sahachko, Yu., Kraliia, V., 2019*). З цієї точки зору ключовою у корпоративному управлінні стає проблема раціонального співвідношення між принципами підзвітності та невтручання власників у діяльність найманих ними вищих керівників, тобто питання корпоративного контролю.

О. Краковський вважає корпоративне управління практикою та вивченням шляхів удосконалення взаємовідносин між різними зацікавленими особами в корпорації. Водночас, за його точкою зору, основна проблема корпоративного управління полягає у створенні механізмів контролю аутсайдерів (кредитори та міноритарні акціонери) над інсайдерами (вище керівництво та акціонери з контрольним пакетом акцій). Таким чином, на його думку, персонал та інші групи учасників корпоративних відносин не беруть активної участі у формуванні та діяльності вищих керівних органів АТ, а тому майже не здатні достатньо впливати на діяльність корпорації. Отже, інтереси цих учасників корпоративних відносин у більшості випадків можуть бути виведені зі сфери корпоративного управління (*Краковський О., 2000*).

Проблему корпоративного управління деякі автори розглядають як проблему гарантування роботи підприємства в інтересах його власників. Зокрема, Д. Коссе і С. Лемма відзначають, що корпоративне управління передбачає механізми, за допомогою яких акціонери компанії здійснюють контроль над робітниками компанії і всім управлінським апаратом в інтересах свого захисту (*Сігер Ч., Паттон Х., 2000*). В свою чергу С. Пишпек формулює корпоративне управління у вузькому та широкому значенні. У вузькому значенні корпоративне управління полягає в забезпеченні діяльності менеджерів по управлінню підприємством в інтересах власників-акціонерів. У ширшому змісті – це захист і врахування інтересів як фінансових, так і нефінансових інвесторів, які вносять свій вклад в діяльність корпорації (*Козаченко А.В. Воронкова А.Є., Є.Н. Коренев., 2001*). М. Озкайа і Х. Аскарі зазначають, що головною метою корпоративного управління є розвиток ефективного моніторингу і спонукальних механізмів, які б скоротили недоліки, пов’язані з виділенням володіння від управління (Синиця С., 1996).

Наступна група авторів підходить до корпоративного управління з позиції взаємовідносин між різними учасниками корпорацій. Так, підхід відомого рейтингового

агентства «Standard & Poor's Corporation» полягає в тому, що корпоративне управління передбачає взаємодію між управляючими компаніями, її радою директорів, акціонерами компанії та іншими фінансовими посередниками (*Баюра Д. О., 2009*). А. Сірош також розкриває корпоративне управління як систему організаційно-правових, економічних і фінансових взаємовідносин всіх учасників підприємства, яка встановлює механізми і методи взаємодії зацікавлених сторін, за допомогою яких вони представляють в підприємстві свої інтереси і взаємодіють з АТ та між собою (*Пишпек С., 2000*).

С. Турнбулл відзначає, що корпоративне управління розкриває процеси в діяльності організації, які пов'язані як з визначенням уповноважених осіб по контролю і регулюванню діяльності, так і з організацією виробництва, реалізацією товарів і послуг (*Сірош Н.В., 1998*).

Деякі автори розглядають корпоративне управління як набір інституційних механізмів, що регулюють відносини між декількома групами учасників у справах діяльності корпорації (інвесторів – як акціонерів, так і кредиторів; менеджерів і робітників) з метою отримання економічних результатів від такої коаліції. М. Чечетов і А. Мендрул розкривають корпоративне управління в широкому значенні як елемент загальної системи управління**,** який притаманний тільки фірмам в організаційно-правовій формі АТ, і полягає в організації взаємодії учасників корпоративних відносин (Turnbull C.S., 2002). Проведене дослідження щодо єдиного визначення корпоративного управління засвідчило, що на даний час його не існує. Однак розкриті точки зору щодо сутності корпоративного управління необхідно узагальнити у розрізі декількох підходів. Г.В. Козаченко пропонує реалізувати це в межах таких підходів: часткового, суспільного, нормативного, економічного та управлінського (*Сігер Ч., 2000*). Але, на нашу думку, запропоновані підходи не охоплюють усю множину визначення корпоративного управління. Автор пропонує впровадити ще два підходи щодо визначення сутності корпоративного управління на основі проведених досліджень: організаційного і інформаційно-економічного та розкрити їх значення (рис. 1.).

Рис. 1. Підходи до визначення сутності корпоративного управління [удосконалено автором на основі джерела (H.Kryshtal, I. Kalina, N.Shuliar, T.Kapeliushna, M.Martynenko, 2022)]

Проаналізувавши усі підходи щодо визначення корпоративного управління та їх сутність, зазначимо, що, на нашу думку, корпоративне управління – спосіб забезпечення захисту і врахування інтересів в нових реаліях як фінансових, так і нефінансових інвесторів, який регламентується нормативно-правовими актами, внутрішніми нормативними положеннями і документами, з метою отримання максимально можливого фінансового

результату.

Аналіз розглянутих понять «корпоративне управління» показує, що його сутність повинна відтворювати, передусім, такі загальні елементи:

- місія, мета та цілі корпоративного управління;
- взаємовідносини між різними групами учасників;
- регламентація цих взаємовідносин як на макрорівні (держава), так і на мікрорівні (конкретного господарського суб'єкта в нових реаліях).

Мета корпоративного управління, яка полягає у підвищенні ефективності функціонування корпорації за рахунок створення балансу інтересів зацікавлених сторін. Досягнення цієї мети є необхідним з точки зору досягнення позитивного економічного розвитку, створення і підтримки сприятливого ділового середовища, забезпечення довгострокового зростання продуктивності та ефективності.

Місією корпоративного управління є забезпечення константного соціально-економічного стану в колективі власників та працівників корпорацій, зокрема, та сприяння дотримання цього статусу в суспільстві (державі) в нових реаліях. Виконання цієї місії здійснюється через систему корпоративного управління, яку доцільно структурувати в окремі автономні підсистеми

Цілі підприємства можуть бути сформульовані однозначно, виходячи з інтересів цього підприємства загалом. Таким чином підприємства та їх учасники майже ототожнюються, а інтереси цих учасників поєднуються на підставі певних чітко визначених внутрішньо організаційних цілей (збільшення прибутку, стабільність виробництва тощо). Проте така тотожність стає можливою, щонайменш, за умови наявності однорідних прав власності та повної відсутності протиріч між власником і найманим персоналом. У великому або навіть у середньому підприємстві виконання зазначених умов є майже неймовірним.

Крім того, внутрішньоорганізаційні цілі великою мірою ґрунтуються на вимогах стабільності існування підприємства та певних стійких взаємовідносинах, що склалися всередині нього. Стратегічні рішення, що базуватимуться на внутрішньоорганізаційних цілях, можуть бути зайво консервативними та зовсім не відповідатимуть умовам господарювання, що безперервно перетворюються. З точки зору власника, навпаки, більш прийнятними здатні ставати стратегії збільшення прибутковості на підставі масштабних змін, здійснення яких руйнуватиме традиційні взаємовідносини та існуючу структуру влади. Таке протиріччя буде виникати, наприклад, при вивченні можливості прийняття стратегічного рішення щодо значного скорочення персоналу. Таким чином, мотивація особи, що проводитиме оцінку доцільності стратегічних рішень, обов'язково має враховуватися при стратегічному

плануванні.

У вузькому розумінні корпоративне управління полягає в забезпеченні діяльності менеджерів щодо управління діяльністю підприємства в інтересах власників. Багато вчених та фахівців розглядають корпоративне управління як методи і способи, за допомогою яких всім зовнішнім інвесторам (акціонерам і кредиторам) гарантовані доходи на їх інвестиції. Деякі дослідники трактують корпоративне управління як захист і врахування інтересів фінансових та нефінансових інвесторів, які роблять свій внесок у діяльність корпорації (концепція співзасновників). Нефінансовими інвесторами вважаються працівники корпорації, що мають специфічний досвід, необхідним саме для цієї корпорації, постачальники, місцеві органи влади.

Корпоративним управлінням вважають систему відносин між органами управління підприємства і його власниками із приводу організації його фінансово-господарської діяльності. Корпоративне управління поєднує норми корпоративного законодавства й корпоративну культуру. Корпоративна культура – це сукупність правил, суспільних норм й усталеної практики в сфері корпоративного управління, що не набула відображення в законодавстві й грунтується на загальному культурному рівні суспільства, прийнятій діловій практиці тощо, стан яких обумовлено рівнем соціально-економічного розвитку країни і, зокрема, фінансового ринку (*Чечетов М., Мендрул А., 2001*).

Дослідження у сфері корпоративного управління мають загальний або міжгалузевий характер. Результати досліджень проблем розвитку підприємств кібербезпеки містять обґрунтування напрямів досягнення ефективності функціонування підприємств на основі маркетингу, використання залучених інвестицій, створення інноваційного середовища.

Корпоративне управління – це взаємозв’язок законодавства й практики організації та керівництва підприємства.

Розглянемо функції корпоративного управління, які на сьогоднішній день є актуальними та забезпечують ефективне функціонування підприємства:

– планування показників фінансово-господарської діяльності підприємства;
– організація фінансово-господарської діяльності підприємства;
– мотивація праці в підприємстві;
– координація основних напрямків фінансово-господарської діяльності підприємства;
– контроль над раціональним використанням ресурсного потенціалу підприємства;
– інноваційна функція;
– маркетингова функція.

Корпоративне управління ґрунтується на принципах, які описані та охарактеризовані:

– принцип централізації корпоративного управління. Перевагами централізації є домінування в процесі ухвалення рішення компетентного кола осіб, усунення дублювання в роботі, зниження управлінських витрат. Недоліки централізації укладаються в можливості концентрації управлінських повноважень у некомпетентних осіб і більших тимчасових витрат при доведенні прийнятих управлінських рішень до конкретних виконавців;

– принцип децентралізації. Первагами децентралізації є швидкість прийняття рішень і доведення їх до виконавців, самостійність низових підрозділів й їхня участь у розробленні та прийнятті управлінських рішень, відсутність необхідності в розробленні детальних планів. Недоліками децентралізації можуть бути: відсутність якості прийнятих управлінських рішень, утруднення уніфікації правил і процедур прийняття рішень;

– принцип координації діяльності структурних підрозділів й окремих працівників;

– принцип ефективного використання ресурсного потенціалу;

– принцип ефективної співпраці з посередницькими структурами, державними організаціями й установами.

Корпоративне управління включає:

– юридичний статус підприємства;

– права учасників на майно підприємства;

– відносини між виконавчими органами й учасниками підприємства;

– роль і повноваження виконавчих органів підприємства;

– організаційну структуру підприємства, правила та порядок його діяльності.

Об’єктом корпоративного управління є корпоративна власність. Корпоративна власність – це, з одного боку, власність корпорації, з іншого боку – власність декількох «великих» або безлічі «дрібних» власників.

Суб’єктами корпоративного управління є: акціонери й інші учасники корпорації; інвестори без права власності; кредитори та інші особи, що володіють зобов’язаннями корпорації; наймані працівники корпорації; господарські партнери корпорації; органи державної влади.

Суб’єкти корпоративного управління одночасно є суб’єктами корпоративних відносин. Корпоративні відносини - це відносини із приводу спільного володіння корпоративною власністю. Суб’єктами корпоративних відносин є: учасники господарських товариств та інших корпорацій; керівництво корпорацій; працівники корпорацій; банки; господарські партнери; держава. Корпоративне управління здійснюється наступними методами: адміністративними; економічними; соціально-психологічними. Адміністративні методи

корпоративного управління базуються на законодавчих актах і нормативних документах, внутрішніх локальних вимогах та правилах і включають методи приказного, розпорядницького впливу на фінансово-господарську діяльність корпоративного утворення. Економічні методи корпоративного управління передбачають використання механізмів економічної й матеріальної зацікавленості суб'єктів корпоративних відносин і включають методи стимулювання якості праці, творчої активності працівників-власників і найманих робітників. Соціально-психологічні методи корпоративного управління пов'язані з реалізацією соціальних інтересів працівників-власників та найманих працівників і включають методи морального заохочення, посадове підвищення (без додаткової надбавки до заробітної платні), присвоєння знаків відмінності, методи об'єктивної оцінки професійних якостей конкретного працівника.

Незважаючи на умови в яких функціонують та розвиваються підприємства, корпоративне управління посідає одне з перших місць, якому приділяють значну увагу, адже при налагодженому корпоративному управлінні підприємство швидко реагує до змін та може пристосуватися, реагує на споживчі цінності та виокремлює їх із тисячі інших, реагує на комунікаційний звязок та ефективно залагоджує споживчі конфлікти тощо.

2. Розробка корпоративної стратегії розвитку підприємств у сфері кібербезпеки в умовах економічної невизначеності.

Діяльність підприємств України на цей час відбувається в умовах швидких непередбачуваних та невизначених змін, як внутрішнього так і зовнішнього оточення. Проявами таких змін стали процеси ринкового реформування економіки, інтернаціоналізація та глобалізація ринків, загострення конкурентної боротьби, безперервне виникнення нових вимог споживачів та новітніх технологій виробництва, кібератак, величезні соціокультурні зміни, а також пандемія Covid-19 та війна (воєнний стан в країні). В цих умовах особливого значення набувають форми та методи стратегічного планування, використання яких дає змогу підприємствам ефективно діяти в будь-яких, навіть самих складних та непередбачуваних, умовах господарювання. Результатом стратегічного планування, тобто організованого процесу розробки та прийняття стратегічних управлінських рішень, стає стратегія підприємства. У більшості теоретичних підходів до стратегічного планування визначається існування відмінностей між інтересами та відповідними до них цілями учасників організації, але вважається, що будь-якого суттєвого впливу на формування стратегії ці відмінності не надають.

Конкурентна позиція підприємства на ринку визначається його конкурентними перевагами, тобто – існуючими порівняльними перевагами підприємств над іншими

підприємствами даної галузі як в всередині та і за межами країни, де відбувається конкурентна боротьба. Наявність певних конкурентних переваг є ознакою рівня конкурентоспроможності підприємств. Рівень конкурентоспроможності підприємств не є постійними характеристиками або ознаками, що заздалегідь задані, а виявляються в певних умовах зовнішнього ринкового оточення та вирішальною мірою залежать від раціональності вибору та успішності реалізації корпоративної стратегії розвитку. Тому характер змін стратегічного потенціалу стає критерієм оцінки ефективності варіантів стратегічних рішень при обґрунтуванні стратегії корпоративного розвитку підприємств. Матриця складається на основі зіставлення двох основних характеристик стратегічного потенціалу підприємств: типу товарного асортименту підприємств, який є найважливішою ознакою ринкових позицій підприємств (вертикальна вісь); питомого обсягу споживання ресурсів на одиницю випуску продукції (доходу) підприємств, тобто узагальнюючого показника ефективності використання всіх видів виробничих ресурсів (горизонтальна вісь). На площині матриці визначено чотири основні сегменти, за якими існуватимуть відмінності у причинах формування та характері стратегічного потенціалу підприємства.

Характеристика основних варіантів стратегічних рішень у сфері корпоративного управління підприємств подана у матриці корпоративних стратегій розвитку (рис. 2). (горизонтальна вісь).

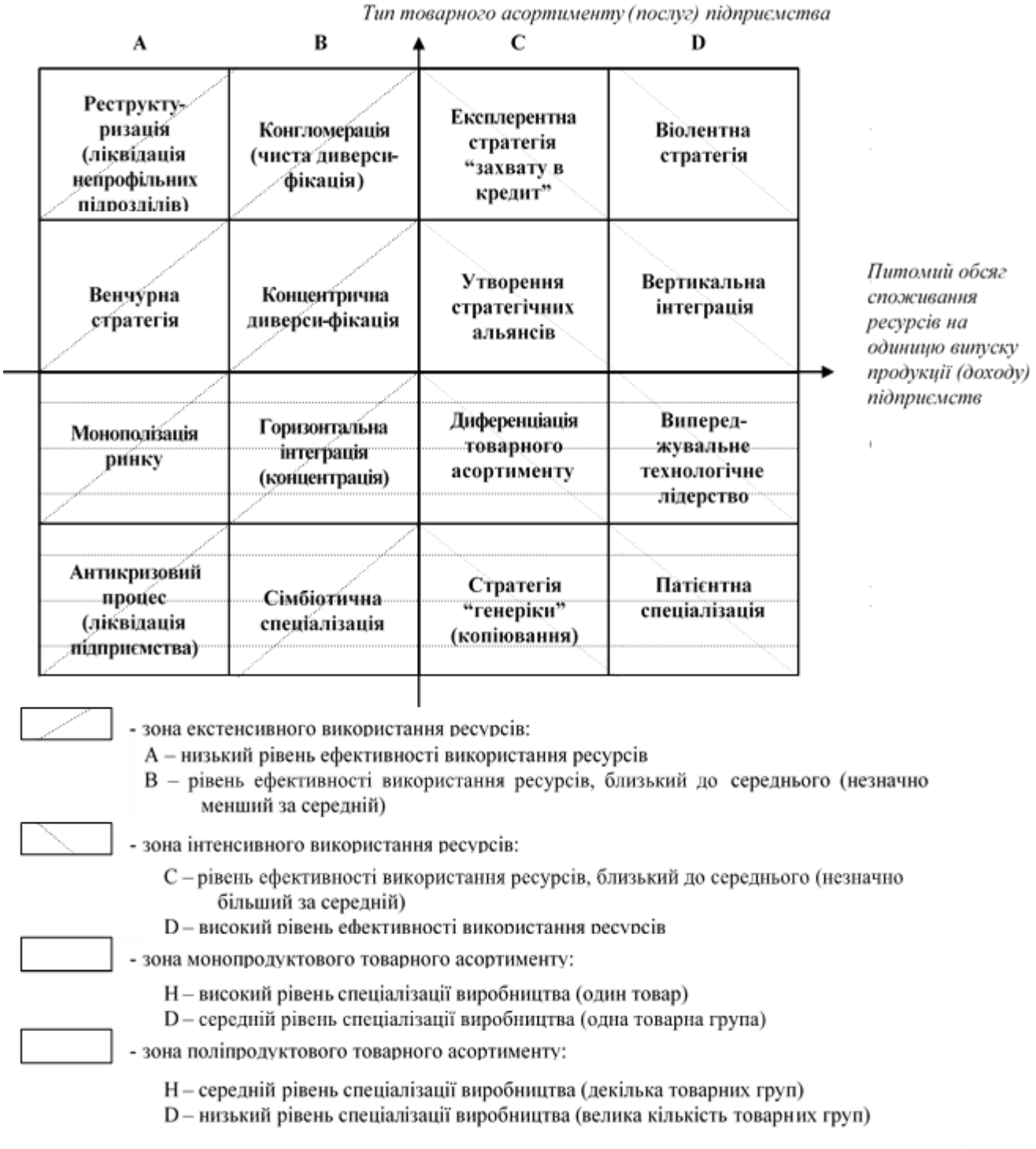


Рис. 2. Варіанти прийняття стратегічних рішень у сфері формування корпоративної стратегії розвитку підприємств [розробка автора]

За ознакою товарного асортименту визначаються зона монопродуктового товарного асортименту (підприємство виготовляє однорідний асортимент продукції, яку призначено для задоволення схожих вимог споживачів на подібних ринках збуту) та зона поліпродуктового товарного асортименту (товари та послуги, що виробляються підприємством, суттєво

відрізняються за потребами, споживачами, ринками збуту або сегментами ринку). За ознакою питомого обсягу споживання ресурсів визначаються зона екстенсивного використання ресурсів (витрати підприємства на виготовлення одиниці продукції або отримання доходу перевищують середні галузеві показники) та зона інтенсивного використання ресурсів (питомі витрати підприємства є меншими за витрати більшості підприємств-конкурентів). Кожна зона за рівнем інтенсивності прояву відповідних ознак, в свою чергу, поділяється на сегменти (A, B, C, D, E, F, G, H).

Перетин певних сегментів матриці визначає причини формування, рівень стабільності стратегічного потенціалу підприємства та відповідну до цих ознак стратегію корпоративного розвитку. Позиціонування підприємства на площині описаної матриці дозволяє дати характеристику стратегічного потенціалу підприємств, обґрунтувати найбільш доцільну стратегію підтримки та розвитку підприємств. Корпоративний розвиток складатиметься у послідовному (за суміжними сегментами) просуванні підприємства до того сегменту матриці (якісного рівня стратегічного потенціалу), який найбільшою мірою буде відповідати цілям сукупності учасників корпоративних відносин.

Проте більшість учасників корпоративних відносин дуже складно однозначно віднести до зовнішнього або внутрішнього середовища. З цієї точки зору, акціонерів-аутсайдерів не можна вважати складовою оточення, оскільки вони як власники підприємства поділяють його загальні інтереси та відчувають від його діяльності стійкий постійний зворотній вплив.

Внутрішнє середовище складається з сукупності факторів, які певною мірою підкоряються внутрішньому контролю та на стан яких підприємство здатне надати прямого та безпосереднього впливу. Вищі керівники та персонал – інсайдери підприємства – в ряді випадків можуть переслідувати власні цілі, обумовлені зовнішніми для інтересів підприємств прагненнями.

За іншими підходами, встановлення стратегічних цілей, спрямованих на задоволення інтересів різних учасників корпоративних відносин, є складовою обраної стратегії підприємства. Проте в такому випадку вихідною посилкою для формування стратегії залишаються внутрішньоорганізаційні цілі, відповідно мірі досягнення яких будуть забезпечуватися прагнення учасників корпоративних відносин. Таким чином, внутрішньоорганізаційні інтереси об’єктивно будуть переважати над фінансовими та суспільними цілями підприємства, що буде неприйнятним для учасників корпоративних відносин – аутсайдерів (*Дмитренко М. Й., 2014*).

Формування корпоративного управління підприємств сфери кібербезпеки через корпоративну стратегію розкрито в рис. 3.

Первинним є те, що корпоративна стратегія формується на будь-якому підприємстві, в нашому досліджені це підприємства в сфери кібербезпеки.

Кібербезпека насправді ще не була чітко визначена, але на практиці вона відноситься до нових викликів, пов’язаних із безпекою, які впливають на організації та суспільство в цілому в міру того, як цифрова трансформація - і наша залежність від взаємопов’язаних цифрових систем і послуг - прогресує.

Кібербезпека також може стосувати заходи, які підприємство може використовувати для захисту своїх критично важливих бізнес-систем, програмного забезпечення, пристроїв і мереж передачі даних від будь-яких кіберзагроз. Кіберзагрози, у свою чергу, - це шкідливі події або процеси, які можуть вплинути на діяльність організації, фінанси, дані, репутацію та, в гіршому випадку, на безперервність її бізнесу (*Баюра Д. О., 2009*).

Автором запропоновано поняття «підприємства у сфері кібербезпеки» це підприємства, які застосовують заходи безпеки з метою забезпечення конфіденційності, цілісності та доступності даних підприємств, яким надають послуги та створюють безпечні товари для захисту цифрового обладнання, інформації та комп'ютерних систем від ненавмисного чи несанкціонованого кібервтручання (кібератак)

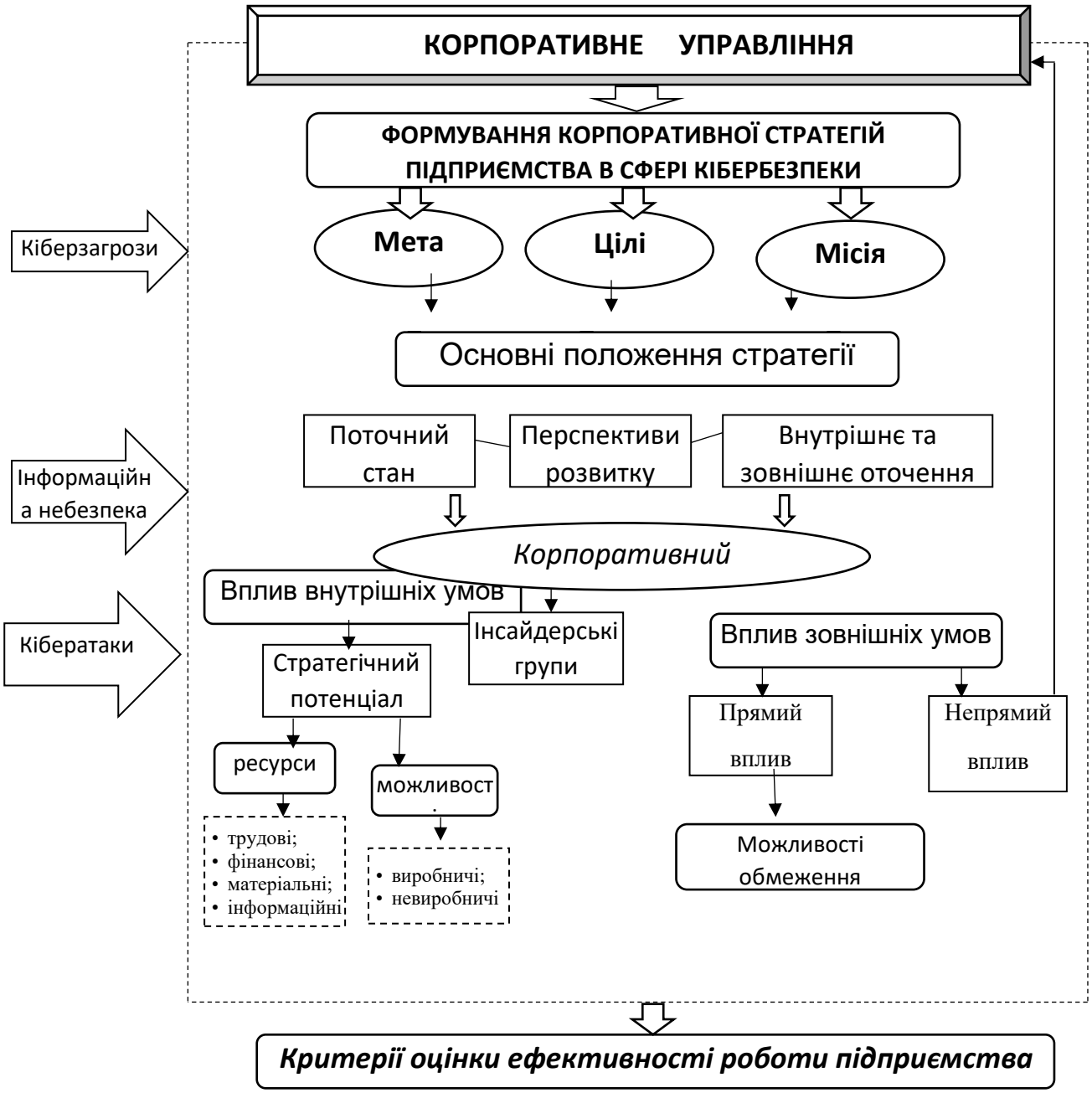


Рис. 3. Формування корпоративного управління підприємств в сфері кібербезпеки [розроблено автором]

Вихідним етапом стратегічного планування корпоративного розвитку є визначення поточного стану, перспектив розвитку зовнішнього оточення та внутрішнього середовища підприємств. Результати оцінки факторів прямого впливу використовуються для визначення можливостей та обмежень операційного оточення підприємства, непрямого впливу – для обґрунтування місії підприємства. Визначення меж операційного оточення підприємства здійснюється для обмеження різноманіття зовнішнього середовища господарювання. До складу операційного оточення належатимуть найбільш впливові зовнішні фактори, перетворення яких здатне надати суттєвого впливу на розвиток підприємств. Результати оцінки стану операційного

оточення надалі використовуються для обґрунтування основних положень корпоративної ділової стратегії та уточнення місії підприємства. Вивчення зовнішнього середовища підприємства також дає змогу встановити склад впливових аутсайдерських груп учасників корпоративних відносин, інтереси яких обов'язково мають враховуватися при «інсайдерському» плануванні діяльності підприємств. Результати оцінки стану та перспектив розвитку внутрішнього середовища підприємства використовуються для визначення її стратегічного потенціалу та складу найвпливовіших інсайдерських груп учасників корпоративних відносин. Розмір та структура стратегічного потенціалу будуть характеризувати наявні ресурсні й виробничі можливості, які матимуть першочергове значення для забезпечення усталеної діяльності підприємства та їх спроможності швидко адаптуватися до змін зовнішніх умов.

Зіставлення можливостей і обмежень операційного оточення та наявного стратегічного потенціалу стає основою для обґрунтування місії підприємства та визначення основних положень корпоративної стратегії .

Необхідність використання місії як загальної бази встановлення цілей при плануванні зумовлено нечіткістю будь-яких конкретних завдань підприємств в наявних умовах прискорення змін і підвищення рівня невизначеності зовнішнього середовища. Проте необхідність забезпечення стабільної діяльності підприємств вимагає подолання невизначеності ринкового оточення через вибір загальних орієнтирів та критеріїв оцінки ефективності роботи підприємства. З цієї точки зору, стратегія стає засобом пристосування внутрішнього середовища корпорації до будь-яких зовнішніх змін з метою повного використання існуючих ринкових можливостей, результати оцінки яких знаходять відбиток у місії.

Деталізація місії підприємств здійснюється через використання традиційних методик стратегічного планування (аналітичного методу, позиціонування тощо). Між прагненнями учасників корпоративних відносин та інтересами підприємства загалом існує складний зв'язок – учасники здійснюють певні внески (фінансові та нефінансові) до діяльності підприємства в розрахунку на отримання відповідної приватної частки від набутих спільних результатів. Проте реальні або передбачувані надходження, які приходитимуться на певного інвестора, можуть виявитися меншими за його очікування. В цьому випадку учасник здатний дійти до висновку про необхідність виходу з корпоративних відносин та виокремлення зробленого ним внеску з корпорації. Таким чином, прийняття певних стратегічних рішень буде призводити до змін інтересів та навіть складу учасників корпоративних відносин. Такі зміни зумовлюватимуть перетворення операційного оточення та стратегічного потенціалу корпорації, тобто призведуть до значної трансформації передумов створення стратегії

корпоративного розвитку.

Таким чином, важливою умовою формування реалістичної корпоративної стратегії розвитку є збалансування основних положень цієї стратегії з прагненнями найвпливовіших груп учасників корпоративних відносин. Склад таких груп (аутсайдерів та інсайдерів) можливо встановити при вивченні зовнішнього та внутрішнього середовища підприємств. Проте визначення переважних інтересів учасників вимагатиме ретельного дослідження та сегментації корпорантів. Таку сегментацію доцільно здійснювати в два етапи: виокремлення угруповань учасників (первинна сегментація); виділення всередині цих угруповань певних груп за інтересами (вторинна сегментація). Вторинна сегментація має здійснюватися за ознакою однорідності інтересів груп учасників та кількісними відмінностями їхніх однорідних цілей.

Практичне втілення настанов, передбачених корпоративною стратегією розвитку, відбувається через ретельне планування усіх аспектів діяльності підприємств на певний період. Особливого значення в системі корпоративного планування має загальний фінансовий план, створений за бюджетним принципом – основний бюджет підприємства. В основному бюджеті здійснюється зіставлення на рівні усього підприємства передбачуваних надходжень грошових коштів та витрат у певному плановому періоді (як правило, на один рік). Важливою перевагою основного бюджету, визначальною з точки зору корпоративного управління, є можливість повної та всебічної оцінки розміру та розподілу результатів діяльності підприємства. В основному бюджеті визначаються усі грошові надходження, які приходяться на користь певних груп учасників корпоративних відносин. Порівняння цих надходжень з приблизними кількісними оцінками очікувань, які передбачено корпоративною стратегією розвитку, надає можливість остаточно визначити відповідність обраної стратегії прагненням учасників корпоративних відносин. В разі значних розходжень між цими показниками, має бути здійснено перевірку раціональності дивідендної політики.

Фінансовий план формується шляхом зіставлення очікуваних у плановому періоді платежів і надходжень. Безпосередньою основою плану є прогнозні розрахунки щодо реалізації продукції споживачам або плани збуту, які складаються виходячи із замовлень, прогнозів попиту й інших факторів ринкової кон’юнктури. Фінансовий план господарської діяльності підприємства може бути укладений двома способами: за бюджетним принципом та як фінансова модель бізнес-плану. Основна розбіжність між цими двома методами полягає в тому, що бюджетний план являє собою підсумок планування соціально-економічного розвитку підприємства й не припускає внесення значних поправок до інших розділів плану, у той час як моделювання бізнес-плану є варіантним і полягає у здійсненні декількох циклів

оптимізації розрахункових показників (*Коваленко Н. В., Панасюк І. В., 2020*).

Іншим можливим способом розробки фінансового плану є фінансове моделювання бізнес-плану. Фінансове моделювання бізнес-плану здійснюється паралельно із плануванням інших аспектів господарської діяльності, є варіантним. Фінансове моделювання бізнес-плану як вихідні передумови припускає ряд припущень, пов'язаних із прогнозом умов господарської діяльності в планованому періоді, а саме: припущення при формуванні маркетингового плану; припущення при розробці виробничого плану; припущення при визначенні плану по продажах; припущення при формуванні плану по розвитку власності; припущення при встановленні варіантів зовнішнього фінансування. Відмінність розглянутих підходів до складання фінансового плану полягає у розбіжності стратегічних цілей і завдань підприємств, покладених до основи при плануванні. Так, планування за бюджетним принципом передбачає переважне урахування факторів, пов'язаних з реалізацією певної конкурентної стратегії. Фінансове моделювання бізнес-плану більшою мірою пов'язане з досягненням або збереженням фінансової стабільності підприємств, забезпеченням дивідендів тощо (*E.Tereshchenko, O. Shkolenko, I. Kosmidailo, I. Kalina, N.Shuliar., 2001).*

Особливе місце в системі стратегічного планування корпоративного розвитку посідає інтеграційна стратегія підприємства. Економічна інтеграція звичайно передбачає встановлення таких взаємин між підприємствами, що забезпечували б довгострокове зближення стратегічних цілей підприємств, які вступають до співробітництва. Таким чином, здійснення процесу економічної інтеграції може передбачати використання широкого кола форм співпраці – від слабкої взаємодії до прямого управління підприємством, яке було поглинене.

Успіх реалізації інтеграційної стратегії підприємства багато в чому залежить від здатності реально оцінити можливості створення вартості в результаті об'єднання маркетингових операційних, дослідницьких та інших потужностей підприємств, що об'єднуються, посилення ринкових позицій, зменшення штату, трансферу технологій тощо (*Spivak, S., Didyk, I., Skurskiy, T. & Zhytko, O., 2001*). Зіставлення загальнокорпоративної стратегії, та аналізу зовнішнього та внутрішнього середовища дозволяє визначити конкретні джерела синергійних ефектів, ймовірність їх досягнення. У найбільш загальному випадку, синергійний ефект, що може бути отриманий під час інтеграції з певним підприємством і може бути виражений у наступному вигляді:

$$\begin{cases} Syn_i = F(A_i; B_i; C_i; \ldots; Z_i) \\ Syn_i \to \max \end{cases}, \quad (1)$$

де Syn_i – загальна синергія, що може бути отримана під час інтеграції з *i*-тим підприємств;

$A_i; B_i; C_i; \ldots; Z_i$ – параметри *i*-того підприємства.

Для отримання максимального ефекту від утворення корпоративного інтеграційного об'єднання синергія має прагнути до максимуму. Тобто, доцільною є інтеграція з тим підприємством, рівень загальної синергії у якого буде більшим.

Для відбору альтернативних варіантів розвитку підприємства доцільним є порівняння синергійних ефектів, що будуть отримані з еталонним. Еталонний синергійний ефект – це максимальний прогнозний ефект, що може бути отриманий під час реалізації всіх заходів, які передбачені інтеграційною стратегією підприємства. Тобто еталонний синергійний ефект – це ефект, що буде отриманий у результаті найбільш ефективної реалізації інтеграційної стратегії даного підприємства, що сформована на основі передумов, які були виявлені під час аналізу діяльності підприємства. Таким чином, доцільною буде інтеграція з тим підприємством, у якого різниця синергійних ефектів буде мінімальна.

Таким чином, формулу 1 можна виразити у наступному вигляді:

$$\begin{cases} Syn_i = F(A_i; B_i; C_i; \ldots; Z_i) \\ Syn_i \to Syn_E \end{cases} \quad (2)$$

де Syn_E – еталонна синергія.

Проте, слід відмітити, що існують виключення з цього правила. Якщо інтеграція з підприємством проводиться для подальшого його продажу, то рівень загальної синергії не буде мати значного впливу. Це обумовлено цілями такої інтеграції та її швидкоплинністю.

Проте, інтеграційні процеси торкаються багатьох аспектів діяльності підприємства та супроводжуються певними витратами на інтеграцію, а також численними ризиками для проведення інтеграційних процесів, для чого пропонується використання показника інтеграційного ефекту:

$$IE_i = Syn_i - TC_i - R_i - AP_i, \quad (3)$$

де IE_i – інтеграційний ефект від утворення з *i*-тим підприємством;

TC_i – загальні витрати на здійснення інтеграції з *i*-тим підприємством;

R_i – ризик, з яким підприємство стикається під час інтеграції з *i*-тим підприємством;

AP_i – альтернативний прибуток, що підприємство втрачає від своєї діяльності.

Загальні витрати на утворення підприємства з корпоративним управління та з ефективною кібербезпекою розраховуються шляхом підсумування всіх витрат, що підприємство буде здійснювати під час інтеграції (див. формулу 1.4).

$$TC_i = \sum_{j=1}^{m} C_j \quad , \tag{4}$$

де C_j - *j*-ті витрати на утворення підприємства;

m – загальна кількість витрат.

Оцінка ризиків корпоративної економічної інтеграції здійснюється за формулою:

$$R_i = \sum_{k=1}^{n} З_K * Y_K \quad , \tag{5}$$

де $З_K$ – збитки, що підприємство може понести під час інтеграції у випадку створення *К*-того небезпечного інформаційного випадку чи кіберзагрози (атаки);

Y_K – ймовірність виникнення *К*-того небезпечного інфомаційного випадку чи кіберзагрози (атаки);

n – загальна кількість небезпечних інформаційних випадків чи кіберзагроз (атак), що може статися під час інтеграції з *i*-тим підприємством;

Отже, інтеграційний ефект від утворення підприємства з *i*-тим підприємством буде дорівнювати:

$$\begin{cases} IE_i = F(A_i; B_i; C_i; \ldots; Z_i) + \sum_{j=1}^{m} C_j - \sum_{k=1}^{n} З_K * Y_{Ki} - AP_i \\ \\ IE_i \to Syn_E \end{cases} \tag{6}$$

Таким чином, дана система рівнянь розкриває сутність синергійного ефекту, що утворюється при формуванні підприємства, та складові такого ефекту. Дана система може використовуватися під час реалізації інтеграційної стратегії підприємств в сфері кібербезпеки для відбору необхідних синергій та виявлення й ліквідації слабких чи незахищених систем інтеграційного чи інформаційного процесу, тобто для запобігання виникненню (інформаційних) перешкод для зростання загального синергійного ефекту до його еталонного значення.

Здійснення описаної послідовності формування корпоративної стратегії розвитку підприємств у сфері кібербезпеки має надати можливості зблизити інтереси різних учасників корпоративних відносин та певною мірою відбити їх у системі планування підприємства. Тільки увага до існування різних інтересів у діяльності підприємства стане основою для покращення стану корпоративного управління, культури корпоративних відносин у вітчизняних підприємств. В подальшому принципи та пріоритети, покладені у формування певних корпоративних стратегій розвитку, мають стати основою для створення кодексів

корпоративного управління підприємств у сфері кібербезпеки та для будь-якого підприємства, яке має бажання захистити комерційну таємницю, персональні дані працівників тощо.

3 Формування організаційно-економічного механізму корпоративного управління підприємств у сфері кібербезпеки.

Корпоративний розвиток являє собою процес стабільно-регулярних, спрямованих, закономірних трансформацій інтересів учасників, а також економічних та духовних передумов і форм корпоративних відносин, які відбуваються під впливом кількісних, якісних та структурних змін в ході корпоративного співробітництва, та джерелом яких стає наростання зовнішніх або внутрішніх протиріч. Тому дотримання вимог стабільності та поступовості корпоративного розвитку обов'язково потребує, з одного боку, реалізації системи заходів із підтримки ефективного корпоративного співробітництва, а, з іншого, – визначає необхідність збалансування цілей корпорантів, а також запобігання загостренню або розв'язання конфліктів в інтересах учасників корпоративних відносин. Вирішення зазначеного широкого кола завдань інституціонального регулювання корпоративних відносин здійснюється на основі формування організаційно-економічного механізму корпоративного управління. Даний механізм являє собою засновану на відносинах власності взаємозалежну сукупність статичної та динамічної складових інституціонального регулювання корпоративних відносин на підприємстві. Організаційно-економічний механізм корпоративного управління визначається індивідуальними та загальними параметрами цілісної сукупності взаємозв'язків між усіма учасниками корпоративних відносин, що виникають навколо процесу прояву та реалізації інтересів корпорантів, а також засобами досягнення цілей в процесі виконання управлінських дій в умовах невизначеності та ризиків.

Трансформаційний ситуативний характер прояву такого роду взаємозв'язків відбиває динамічний аспект побудови і розвитку системи корпоративних відносин, а також великою мірою визначає сприйнятливість нормативного забезпечення корпоративних відносин до змін умов господарювання. Даний механізм як організаційний елемент складного явища – механізму корпоративного управління – на рівні підприємства встановлює принципи і визначає особливості структурної побудови корпоративного управління, розподілу відповідальності, влади і компетенцій, сприяє досягненню збалансованості статичного і динамічного аспекту інституціонального регулювання.

У сфері корпоративних відносин явищем, виникнення якого започатковує функціонування організаційно-економічний механізм корпоративного управління, безумовно, слід вважати конкретизацію та формалізацію інтересів корпорантів при здійсненні процедур індивідуального та колективного вибору певних моделей і стратегій поведінки. В ході

реалізації такого роду процедур відбувається погодження різноспрямованих прагнень учасників корпоративних відносин, встановлюються прийнятні умови досягнення консенсусу між різними зацікавленими групами, визначаються гарантії забезпечення дотримання законних прав корпорантів тощо. Надалі широке розгортання безпосередньо процесу корпоративного співробітництва закономірно призводить до завершального етапу даного циклу розвитку механізму, ознакою настання якого стає отримання проміжних (або остаточних) результатів управлінської діяльності в сфері корпоративних відносин, що можуть бути зіставлені із вихідними очікуванням корпорантів.

Організаційно-економічний механізм корпоративного управління підприємств має виконувати, на думку автора, наступні завдання:

1) орієнтуватися на досягнення кінцевої стратегічної мети при виборі корпоративного управління;

2) удосконалювати методики та техніки підготовки і прийняття управлінських рішень;

3) розробляти та впроваджувати системи показників ефективності функціонування об’єкта.

Основна мета організаційно-економічного механізму корпоративного управління підприємств полягає у забезпеченні цілеспрямованого оперативного регулювання діяльності за напрямами корпоративного управління для забезпечення відповідності фактичного стану підприємства цільовим параметрам.

Автор вважає, що формування механізму передбачає охоплення широкої сфери корпоративних відносин, пов’язаної із урахуванням дії множини факторів і чинників зовнішнього і внутрішнього походження. Безпосередніми передумовами для розбудови організаційно-економічного механізму корпоративного управління виступають економіко-правовий механізм забезпечення інтересів та фінансовий механізм забезпечення інтересів учасників корпоративних відносин, мотиваційний механізм корпоративного співробітництва підприємства, механізм формування та розподілу корпоративного контролю підприємства.

При цьому слід підкреслити, що особливість ролі та функцій механізму полягає в тому, що правила прямо не визначають процедури прийняття або зміст конкретних управлінських рішень, реалізація яких безпосередньо пов’язана зі зміною стану факторів або із перетворенням ресурсів корпоративного управління. Правила внутрішньокорпоративного походження описують умови і домовленості, на які погоджуються учасники при вступі до корпоративного співробітництва. При цьому такого роду умови можуть досить чітко і жорстко визначати обмеження, в рамках яких надалі буде відбуватися формування конкретних

процедур корпоративного управління. Складові механізму відображають сукупність ціннісних установок, норм, формальних та неформальних законів поведінки, які відбивають стан соціальних, економічних, виробничих відносин, що склалися в корпоративній організації та культивуються найбільш впливовими учасниками корпоративного співробітництва.

Організаційно-економічне забезпечення складається із системи цілей і стратегій, які базуються на балансі інтересів учасників корпоративних відносин. З іншого, – нормативно-правове забезпечення, яке виступає найважливішою формою унормування конкретних корпоративних ситуацій, які виникають в процесі розвитку підприємства.

При цьому слід підкреслити, що особливість ролі та функцій механізму полягає в тому, що правила прямо не визначають процедури прийняття або зміст конкретних інформаційно-управлінських рішень, реалізація яких безпосередньо пов'язана зі зміною стану факторів або із перетворенням ресурсів корпоративного управління. Правила внутрішньокорпоративного походження описують умови і домовленості, на які погоджуються учасники при вступі до корпоративного співробітництва. При цьому такого роду умови

можуть досить чітко і жорстко визначати обмеження, в рамках яких надалі буде відбуватися формування конкретних процедур корпоративного управління.

В положеннях нормативно-правового забезпечення, як складової механізму, знаходить відображення сукупність ціннісних установок, норм, формальних та неформальних законів поведінки, які відбивають стан соціальних, економічних, виробничих відносин, що склалися в підприємстві та культивуються найбільш впливовими учасниками корпоративного співробітництва.

Розглянемо більш детально організаційно-економічнй механізм корпоративного управління підприємств в сфері кібербезпеки, який поєднує три блоки: нормативно-правове забезпечення (з урахування оновлення та відсутності нормативно-правових актів), організаційно-економічне забезпечення (з відповідним ресурсним забезпечення та з урахуванням зовнішніх на внутрішніх факторів), інформаційно-управлінське забезпечення (з урахування особливостей підприємства, інформації, яка надходить до підприємства та виходить з нього та пріоритетів розвитку корпоративного управління). Кожен блок механізму є універсальним та доповнює один одного, без нормативного-правового блоку ефективно не функціонуватиме як організаційно-економічний так і інформаційно-управлінський, адже не буде правової основи для налагодженн звязків між підприємствами та споживачати та незможе підприємство себе захистити (як інформаційному просторія, так і на фізичному рівні). В сукупності забезпечує особливості створення й функціонування механізму, в індивідуальності й інтегральній єдності таких елементів. Складові організаційно-економічного механізму

корпоративного управління підприємств в сфері кібербезпеки представлено на рис. 4.

А також у досягненні запланованих перспективних економічних і соціальних результатів. У межах соціально-етичних і юридичних норм, прийнятих в суспільстві, дія правил проявляється в особливому стилі поведінки, який об'єднує або розмежовує корпорантів в процесі досягнення спільних стратегічних та поточних цілей. Положення певної базової корпоративної угоди визначальним чином впливають на поведінку учасників корпоративних відносин та їхні реакції на будь-які зміни в корпоративному співробітництві. Основними характеристиками прояву механізму стає визначення вимог до наступних параметрів участі корпорантів у корпоративні відносини: особиста ініціатива та рівень толерантності учасників; готовності до прийняття певних корпоративних ризиків; цілеспрямованість, узгодженість і управлінська підтримка спільних дій; правила контролю, координації та взаємодії; ідентичність корпоративної організації та її учасників; система мотивації тощо.

Рис.4. Складові організаційно-економічного механізму корпоративного управління підприємств в сфері кібербезпеки [розроблено автором]

Іншими важливими функціями механізму в процесі функціонування та розвитку корпоративного управління стає формування певного образу підприємства та забезпечення соціальної стабільності, єдності й відданості корпорантів.

Механізм такого роду не є цілком однорідним явищем – для більшості сучасних великих підприємств притаманним є існування домінуючої парадигми внутрішньокорпоративного інституціонального регулювання та декількох субкультурних утворень, що виникають в її межах.

Субкультури виявляються за умови необхідності адаптації окремих учасників корпоративного співробітництва до певної специфіки діяльності або територіальної диференціації. Важливу роль в процесі забезпечення сталого корпоративного співробітництва відіграють також методи соціалізації, які допомагають новим учасникам адаптуватися до внутрішньокорпоративного середовища. До найбільш переконливих способів соціалізації належать історії та легенди, ритуали, символи успіху, специфічна мова й прийоми спілкування. допомагають новим учасникам адаптуватися до внутрішньокорпоративного середовища. Послідовність формування організаційно-економічного механізму корпоративного управління підприємства представлено на рис. 5.

Таким чином, формування базової корпоративної угоди, що являє собою складне сполучення інституціональних норм обмежуючого та спонукального характеру є невід'ємною складовою забезпечення ефективного функціонування механізму. Наявність серед корпорантів погодженого усвідомлення спільних цілей і цінностей, єдність та взаєморозуміння, що ґрунтуються на ідеологічних засадах корпоративізму, суттєво розширюють можливості для підвищення результативності спільної діяльності.

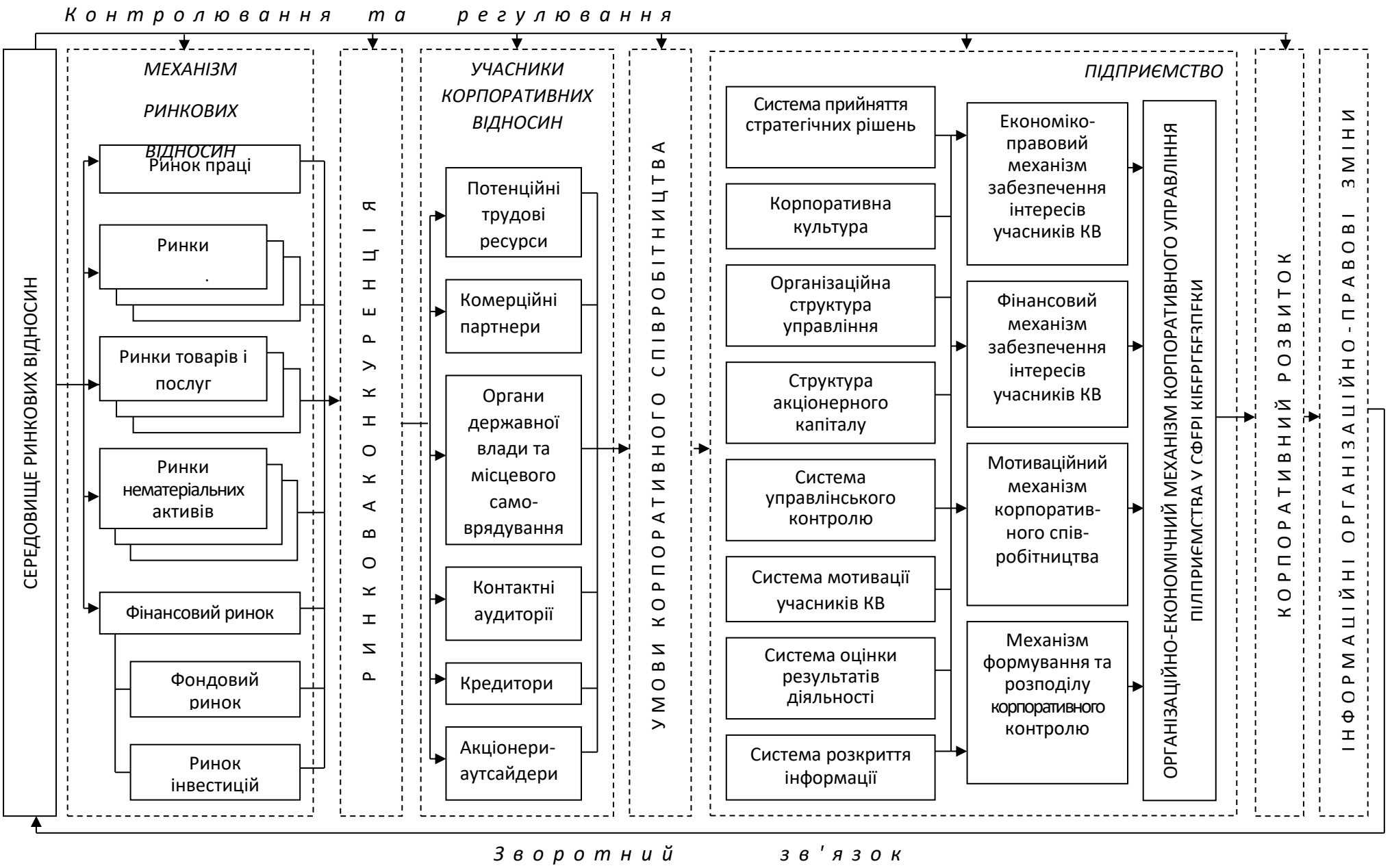


Рис.5. Послідовність формування організаційно-економічного механізму корпоративного управління підприємства [розроблено автором]

ВИСНОВОК

Отже, сучасна парадигма корпоративного управління, що передбачає достатньо виважене врахування базових елементів, дає змогу визначати теоретичні засади в нових реаліях, які проголосили курс на формування відносин в цифровому середовищі. Цифровізаційні тенденції не тільки підвищили ефективність функціонування підприємства, а й призвели до значного збільшення фінансових, інформаційних та трудових ресурсів для забезпечення безпеки від проникнення (кібератаки) та захисту інформації, систем та платформ. Для ефективного функціонування підприємства та корпоративного управління потрібно впроваджувати стратегію, яка є допоміжним елементом (складовою) розвитку. Таким чином, важливою умовою формування реалістичної корпоративної стратегії розвитку є збалансування основних положень цієї стратегії з прагненнями найвпливовіших груп учасників корпоративних відносин. Найважливішими чинниками забезпечення збалансованості і погодженості сполучення складових організаційно-економічного механізму та їх динамічного походження стають правила здійснення корпоративних відносин на підприємстві в небезпекових умовах. З одного боку, на ґрунті встановлення та забезпечення неухильного дотримання правил базової корпоративної угоди відбувається узгодження організаційно-методичного та інструментального забезпечення корпоративного управління із системою цілей і стратегій корпорантів, які базуються на балансі інтересів учасників корпоративних відносин. З іншого, – нормативно-правове забезпечення, яке виступає найважливішою формою унормування конкретних корпоративних ситуацій, які виникають в процесі розвитку підприємства.

References:

Євтушевський В.А. (2002). Основи корпоративного управління: Навч. посіб. К.: Знання-Прес, 2002. 317 с.

McConnell K.R., Brew S.L. (1998). Economics: Principles, Problems and Policy. Translated from English. Revised Edition 11. K., HaGar, 1998. 785 p

Richard J. Teweles, Edward S. Bradley. (1998). The Stock Market 7th Edition. McGraw Hill.1998. 576 pages

Paul Samuelson,William Nordhaus (2009). Economics 19th Edition. McGraw Hill. 2009. 744 pages

Marshall, J. and V.K. Bansal (1992). Financial Engineering: A Complete Guide to Financial Innovation, New York Institute of Finance, New York.

H. Igor Ansoff(1988). The New Corporate Strategy. John Wiley & Sons. 1988. 241 pages

Тарасюк А.В. (2017). Відкриті дані та інші дані у публічному доступі : правові аспекти // Інформація і право. № 2(21)/2017. С. 59-65.

Господарський кодекс України Верховна Рада України; Кодекс України № 436-IV 16.01.2003. редакція 19.08.2022, підстава - 2479-IX

Гриньова В.М., Попов О.Є. (2003). Організаційно-економічні основи формування системи

корпоративного управління в Україні. Монографія. Х.: Видавництво ХДЕУ, 2003. 324 с.
Краковський О. Корпоративне управління після масової приватизації. Перспективи для України. Круглий стіл Евразії з корпоративного управління (під патронажем КМУ). Київ, Україна 19-20 жовтня 2000 рік (зб. матеріалів)
Сігер Ч., Паттон Х. (2000). Загальний стан та передумови розвитку фінансового ринку в Україні. Financial Markets International, Inc. 2000 191 с.
У пошуках кращого директора: Корпоративне управління в перехідній та ринковій економіках: Пер. з англ..; Наук. ред. С. Синиця. К.: Основа, 1996. 189 с.
Козаченко А.В. Воронкова А.Є., Є.Н. Коренев (2001). Основи корпоративного управління: Навч. посібник. Східноукраїнський національний ун-т. – Луганськ: ВНУ, 2001. 480 с.
Пишпек С. (2000). Про ефективне управління корпоративною власністю. Економіка України. 2000. №4. С. 86-88.
Сірош Н.В. (1998). Формування корпоративного сектора економіки в Криму і деякі проблеми корпоративного управління // Державний інформаційний бюлетень про приватизацію бюллетень о приватизации. 1998. №5. С. 37-41.
Turnbull C.S. (2002). Corporate Governance An International Review 10(4):261-277. 2002. DOI:10.2139/ssrn.316939
Чечетов М., Мендрул А. (2001). Корпоративне управління в умовах економічної трансформації. Економіка україни. 2001. №4. С. 10-18.
Корпоративна культура: біхевіоральний і праксеологічний аспекти / М. Й. Дмитренко // Вісник Житомирського державного університету імені Івана Франка. 2014. Вип. 5. С. 3–7.
Баюра Д. О. (2009). Система корпоративного управління в Україні: стан та перспективи розвитку: монографія/ Д. О. Баюра. К.: Видавничо-поліграфічний центр «Київський університет», 2009. 288 с.
H.Kryshtal, I. Kalina, N.Shuliar, T.Kapeliushna, M.Martynenko, (2022). IngramTrends of development of financial and economic activity of entrepreneurial structures during the period of quarantine restrictions. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 2022, № 1, pp. 139-144 (Scopus)
Коваленко Н. В., Панасюк І. В. (2020). Управління ризиками транснаціональних корпорацій. Економіка та менеджмент кораблебудування №4, 2020 С. 103-109. http://dx.doi.org/10.15589/znp2020.4(482).12
Eleonora Tereshchenko, Oksana Shkolenko, Inna Kosmidailo, Iryna Kalina, Nataliia Shuliar (2021). Formation of an effective risk management system at the enterprise. Фінансово-кредитна діяльність: проблеми теорії і практики (Financial and credit activity-problems of theory and practice) 1/2021 pp320-329. URL: http://fkd.org.ua/issue/view/13824
Spivak, S., Didyk, I., Skurskiy, T. & Zhytko, O. (2021). Rol kompiuternykh prohram dlia analizu finansovo-hospodarskoho stanu pidpryiemstva. Sotsialno-ekonomichni problemy i derzhava [Socio-Economic Problems and the State] (electronic journal), Vol. 25, no. 2, 2021 pp. 702-707. Available at: http://sepd.tntu.edu.ua/images/stories/pdf/2021/21ssmgsp.pdf
Dudnyk, O., Sahachko, Yu., Kraliia, V. (2019). Planning of the organizational structure of the enterprise management in the conditions of implementation innovative technologies of production and technological changes. Innovative tools for socio-economic systems' development. Series of monographs Faculty of Architecture, Civil Engineering and Applied Arts Katowice School of Technology Monograph 25. 2019р. 25-34
Воронкова А. (2006). Корпоративне управління та культура: (Монографія) / А.Е. Воронкова, М. М. Баб'як, Е. Н. Коренєв, І. В. Мажура. Дрогобич: Вимір, 2006. 376 с. Бібліогр.: с. 332-352.
Гриньова В.М., Попов О.Є. (2003). Організаційно-економічні основи формування системи корпоративного управління в Україні. Монографія. Х.: Видавництво ХДЕУ, 2003. 324 с.

Краковський О. (2000). Корпоративне управління після масової приватизації. Перспективи для України. Круглий стіл Евразії з корпоративного управління (під патронажем КМУ). Київ, Україна 19-20 жовтня 2000 рік (зб. матеріалів)
Корпоративна культура: біхевіоральний і праксеологічний аспекти / М. Й. Дмитренко // Вісник Житомирського державного університету імені Івана Франка. 2014. Вип. 5. С. 3–7.
Пономаренко В. (2006). Корпоративне управління машинобудівним підприємством: проблеми, шляхи вирішення: (Монографія). /В.С. Пономаренко, Є.М. Ястремська, В.М. Луцьківський, С.Л. Кушнар, Д.А. Ріпка, Н.В. Бєлікова. Х. ВД «ІНЖЕК», 2006. 232 с.
Арістова В. І., Сулацький Д. В. (2013). Інформаційна безпека людини як споживача телекомунікаційних послуг. К. Право України; Харків. Право. 2013. 184 с.
Арсенович Л. А. (2021). Організація професійної підготовки фахівців із кібербезпеки основними суб'єктами національної системи кібербезпеки: практичний аспект. Ефективність державного управління, (62). https://doi.org/10.33990/2070-4011.62.2020.205817
Л. Кириченко, Т. Радівілова, А. Карлссон (2018). «Виявлення кіберзагроз за допомогою аналізу соціальних мереж: коротке опитування». CoRR abs/1805.06680.

DOI 10.5281/zenodo.10820587
UDC 336.1(477.74-72).012.334

CHAPTER 9.
FORMATION OF A FINANCIAL CLUSTER FOR THE DEVELOPMENT OF THE TERRITORIAL COMMUNITIES OF ODESCHA

Victoria KOVALENKO
D.Sc. in Economics, Professor
Odesa National University of Economics, Department of Banking
(8 Preobrazhenskaya Str., Odesa, 65082, Ukraine)
kovalenko-6868@ukr.net
https://orcid.org/0000-0003-2783-186X

Abstract. The paper describes the channels of financial support for the development of territorial communities. The main forms of investment and credit support for the development of territorial communities include: state support, bank lending and investment. The financial capabilities of the Odesa region's banking services market to stimulate the development of territorial communities have been determined. The theoretical and methodological basis for the creation of financial clusters to ensure the development of territorial communities has been formed. It is proven that the system of financial and credit, organizational and legal regulation of the functioning of financial clusters additionally requires such levers of influence as budgetary, tax, monetary, currency, investment, price, financial levers of local self-government bodies/

Keywords: territorial communities, banks, regional market of banking services, credit and investment support, financial cluster, financial support.

ФОРМУВАННЯ ФІНАНСОВОГО КЛАСТЕРУ ДЛЯ РОЗВИТКУ ТЕРИТОРІАЛЬНИХ ГРОМАД ОДЕЩИНИ

Анотація. У роботі надано характеристику каналів фінансової підтримки розвитку територіальних громад. До основних форм інвестиційно-кредитного забезпечення розвитку територіальних громад віднесено: державна підтримка, банківське кредитування та інвестування. Визначено фінансові можливості регіонального ринку банківських послуг Одещини для стимулювання розвитку територіальних громад. Сформовано теоретико-методичне підґрунтя створення фінансових кластерів для забезпечення розвитку територіальних громад. Доведено, що система фінансово-кредитного, організаційного та

правового регулювання функціонування фінансових кластерів, додатково вимагає таких важелів впливу як бюджетних, податкових, монетарних, валютних, інвестиційних, цінових, фінансових важелів органів місцевого самоврядування.

Ключові слова: територіальні громади, банки, регіональний ринок банківських послуг, кредитно-інвестиційне забезпечення, фінансовий кластер, фінансова підтримка.

Вступ. Сьогодні як ніколи актуалізується питання щодо нейтралізації дисбалансів у розвитку регіональних ринків банківських послуг, які викликані як саме присутністю на території банків - юридичних осіб, станом економічного розвитку регіону та фінансовими можливостями для стабільного функціонування територіальних громад.

Зазначене ускладняється подіями введення воєнного стану в Україні, подовженням сплесків пандемії COVID 19, значними руйнуваннями у громадах та критичної інфраструктури. Все це вимагає пошуку альтернативних джерел фінансування для відновлення територій, пошуку дієвих механізмів інвестиційної підтримки соціально-економічного розвитку регіонів. Саме тому, актуалізується питання щодо оцінювання можливостей регіонального ринку банківських послуг щодо формування фінансового кластеру для визначення стратегічних напрямів відновлення та подальшого розвитку територіальних громад, виходячи з того, що банки залишаються рушійною силою у подоланні негараздів у соціальній, економічній та інвестиційно-інноваційній сфері.

Постановка проблеми. Подальшого дослідження потребує питання пошуку ефективних рішень щодо визначення пріоритетних напрямів фінансово-інвестиційної підтримки розвитку територіальних громад з боку саме банківських установ, особливо під час дії воєнного стану та у повоєнний час. Також за необхідне є розробка механізму, який надає можливість створення фінансового кластеру, функціонування якого у регіональному розрізі сформує необхідні фінансові важелі для відбудови та соціально-економічного розвитку територіальних громад.

Аналіз останніх досліджень і публікацій. Аналізу впливу розвитку регіональних ринків банківських послуг присвячені наукові праці З. Герасемчук та О. Гоманюк, які визначили фактори впливу на розвиток регіональних ринків банківських послуг, а саме: територіальні, соціально-демографічні, культурно-історичні, економічні, політично-правові та організаційні (*Герасимчук З.В., Гоманюк О.К., 2015*). Також заслуговує на увагу наукова праця колективу авторів О. Гасія, А. Соколової та Н. Прохар, у якій визначено фактори конкурентного середовища регіональних банківських систем. До них віднесено публічне управління на рівні регіону, пропозиція банківських продуктів у регіоні, умови функціонування банків різної

форми власності у регіоні, рівень розвитку інвестиційної діяльності банків, аутсорсинг банківських та партнерських продуктів, рівень діджіталізації банків, рівень розвитку економіки та фінансової грамотності населення та інші (*Гасій О. В., Соколова А.М. та Прохар Н. В, 2021*).

Також серед наукових здобутків щодо розвитку ринку банківських послуг слід віднести напрацювання В. Чалої, яка запропонувала головні продукти і сервіси зеленого банківництва (зелені банківські кредити, зелене страхування, сек'юритизація, інвестиції в основний капітал, брокерська діяльність та технічна допомога (*Чала В. С., 2021*). Представлені компоненти викликають значну зацікавленість для фінансово-економічної підтримки територіальних громад.

У подальшому, слід звернути увагу на публікації, які зосереджені саме на проблемах розвитку територіальних громад. З цього питання заслуговують на увагу наукові здобутки Є. Мураєва *(Мураєв Є., 2020),* О. Польової *(Польова О., 2020)*, М. Ажажи, О. Фурсін та О. Венгер *(Ажажа М., Фурсін О., Венгер О., 2022)*, Р. Содоми *(Содома Р., Дубневич Ю., Марків Г. та Шматковська Т., 2021)*.

Серед наукових доробок, які присвячені проблематиці теоретико-методологічним засадам формування фінансових кластерів слід відміти дослідження, які проведені Н. Зарічною (*Зарічна Н.З., 2021*), П. Пузирьової (*Пузирьова П., 2019*), О. Попело та співавтори (*Попело О., Бутко М., Ревко О., Гарафонова О. та Розповідей О.*).

Характеристика каналів фінансової підтримки розвитку територіальних громад.

Основною характеристикою стану територіальної громади є соціально-економічний розвиток території, на якій вона функціонує. У науковій праці Р. Содоми (*Содома Р., Дубневич Ю., Марків Г. та Шматковська Т., 2021*) , визначено структурні елементи ресурсної бази соціально-економічного розвитку територіальних громад, а саме: людські ресурси, фізичні ресурси, нематеріальні активи, інституції, матеріальні об'єкти, природні ресурси та фінансові ресурси.

У цьому контексті заслуговує на увагу дослідження проведене Є. Мураєвим, який запропонував модель прогнозно-аналітичної системи оцінки рівня збалансованого розвитку розумних міст за збалансованою системою показників розумного міста, реалізація якої забезпечуватиметься за такими сферами діяльності: розумні люди, розумне урядування, інформаційно-комунікаційні технології, технологія та інфраструктура, розумна економіка, якість життя та комфорту в місті (*Мураєв Є., 2020*), (табл. 1).

Таблиця 1

Модель прогнозно-аналітичної системи оцінки рівня збалансованого розвитку розумних міст за збалансованою системою показників розумного міста (Smart City Balanced Scorecard (SCBSC0

Якість життя	Якість життя та комфорту в місті	Транспорт	Безпека	Довкілля
		Охорона здоров'я	Освіта	Культура та інформаційна політика
Цифрова економіка	Розумна економіка	Безготівкові розрахунки	Електронна комерція	Міжнародна інтеграція
		Фінансування	Інвестиції	Інновації
Технологічні інновації	Технологія та інфраструктура	Енергія	Розумне житло	ЖКГ
	ІКТ	Цифрова інфраструктура	Телекомунікації	Соціальні мережі
Розумні люди та урядування	Розумне урядування	Партнерська екосистема	Якість адміністрування процесів	Підзвітність і прозорість влади
	Розумні люди	Е-урядування	Міське планування	
		Людський капітал	Цифрові навички	Соціальна згуртованість

Джерело: (*Мураєв Є., 2020*),

М. Ажажа, у цьому напрямку виокремлює три основних компоненти розвитку територіальних громад:

Інновації як конкурентна перевага регіонального економічного розвитку та їх роль у формуванні інноваційної екосистеми;

Напрями розвитку інноваційної та креативної державної політики;

Концептуалізація побудови інноваційних екосистем розумного міста;

Інновації, екосистема та місцеве самоврядування (*Ажажа М., Фурсін О., Венгер О., 2022*).

Як ми бачмо, запропоновані заходи вимагають в першу чергу розробки певних напрямів щодо фінансової підтримки, яка акумулюється на регіональних ринках банківських послуг.

До об'єднаних громад області відносяться Березівський район, Білгород-Дністровський район, Болградський район, Ізмаїльський район, Одеський район, Подільський район, Роздільнянський район.

Найбільш постраждалим виявився з часу воєнних дій в Україні Білгород-Дністровський район, а саме: смт Затока Кароліно-Бугазької сільської територіальної громади, с. Біленьке Шабівської сільської територіальної громади, смт Сергіївка Сергіївської селищної територіальної громади, с. Тузли Тузлівської сільської територіальної громади.

За підтримки уряду Великої Британії, обрано 10 громад, які розпочнуть процес відновлення. Загалом заявки на участь надіслали 487 українських громад, які постраждали внаслідок російської агресії. До складу учасників увійшли Вінницька область (Ладижинська громада), Миколаївська область (Новобузька громада), Одеська область (Кароліно-Бугазька громада), Полтавська область (Гоголівська громада), Сумська область (Роменська та Дубов'язівська громади), Харківська область (Новопокровська громада), Чернігівська область (Сосницька, Бобровицька та Михайло-Коцюбинська громади) (*Децентралізація, 2024*).

З 2014 році в Україні здійснюється комплексна реформа місцевого самоврядування та територіальної організації влади на засадах децентралізації. Міжнародна спільнота послідовно підтримує цю реформу і виділяє значні ресурси на її впровадження по всій території країни, і продовжує робити це навіть під час війни (табл. 2).

Таблиця 2

Список проєктів та програм міжнародної технічної підтримки

Проєкт	Області	Громади	Дата початку	Дата закінчення	Сума
Програма U-LEAD	Усі області	Усі громади	01.01.2016	31.12.2023	176 млн EUR
Проєкт USAID "ГОВЕРЛА"	12	101	19.03.2021	20.03.2026	74 млн USD
Програма Ради Європи	Усі області	Усі громади	01.01.2023	31.12.2024	1,4 млн EUR
Проєкт DECIDE	5	20	01.02.2020	31.05.2025	11,7 млн CHF
SALAR International	Усі області	Усі громади	08.09.2014	31.01.2024	79,95 млн SEK
Проєкт PROSTO	Усі області	Усі громади	13.09.2021	31.01.2024	47 млн SEK
Проєкт SURGe	12		01.10.2019	31.12.2024	не має даних

Джерело: *(Децентралізація, 2023).*

Перелік грантових проектів, які дають додаткові можливості для громад у 2021 р. наведено у таблиці 3.

Таблиця 3

Грантові можливості для територіальних громад у 2024 році

№ пор	Назва проєкту, посилання
1.	Грантова програма «Культура, регіони» УКФ (до 3 млн грн) http://surl.li/psbsv
2.	Фінансування будівельних робіт в рамках програми «Відновидім» (до 7,2 млн грн) http://surl.li/qosqt
3.	Другий конкурс проєктних пропозицій Дунайської регіональної програми (38,7 млн євро) http://surl.li/qeupj
4.	Грань «Системи кластерів управління відходами у малих та середніх громадах України» USAID "ГОВЕРЛА" (1 млн дол США) http://surl.li/pudwi
5.	Гранти для малих та середніх проєктів в рамках програми INTERREG NEXT Румунія – Україна (Малий проєкт "Транскордонний екологічний фокус" - 5670964 євро; Малий проєкт "Транскордонний соціальний розвиток" - 9996282 євро; Малий проєкт "Транскордонне співробітництво" - 2412947 євро; Середній проєкт "Транскордонний соціальний розвиток" – 12666237 євро. http://surl.li/qosvc
6.	Грант на розробку інвестиційних концепцій від ІД EUCF (60 тис євро) http://surl.li/qoswf
7.	Міні-Грант «Здорові рішення для відкритого суспільства» (50 тис грн) http://surl.li/qosxe
8.	Гранти на поліпшення кібербезпеки державних установ та об'єктів критичної інфраструктури України. CRDF Global за підтримки Державного департаменту США. http://surl.li/qosxw
9.	Співфінансування створення навчального центру USAID АГРО – підготовка професійних кадрів у секторах зберігання та переробки зернових та олійних. (до 11 млн дол США). http://surl.li/qekwl
10.	Грантовий конкурс для проєктів у сфері «Зеленої» енергетики (до 10 тис. євро) http://surl.li/qoszm
11.	Співфінансування для модернизації меліоративної інфраструктури організацій водокористувачів від USAID АГРО (18,35 млн грн) http://surl.li/qotai
12.	Конкурс на участь у швейцарсько-українській програмі «Згуртованість та регіональний розвиток України» UCORD http://surl.li/qotbl
13.	Конкурс ініціатив, що сприяють верховенству права WORLD JUSTICE CHALLENGE 2024 (до 20 тис дол США) http://surl.li/qotbv
14.	Програма «Цифрова трансформація в публічному врядуванні» від МІНЦИФРИ http://surl.li/qotcn
16.	Фінансування проєктів з енергоефективності громадських будівель (для громад та середніх і малих міст України) (100 млн євро) http://surl.li/qotda
17.	Для громад на проєкти з відновлювальної енергетики. Громадські організації Екоклуб, Екодія, Energy Act For Ukraine Foundation, RePower Ukraine спільно з GIZ за дорученням Уряду Німеччини (30-50 тис євро) http://surl.li/qotff

Джерело: (*Центр розвитку «Час змін», 2024*)

Слід звернути увагу на відсутність в Україні достатнього обсягу конструктивного капіталу, який можна спрямовувати на відновлення (табл. 4).

Таблиця 4

Оцінка розподілу українського капіталу за типами, %

Вага	Категорія	Іноземний конструктивний	Іноземний корозійний	Державний	Комунальний	Олігархічний	Інший корозійний	Конструктивний	До визначення
28	300 найбільших компаній за виторгом	10	4	22	1	28	6	12	17
58	Інші компанії	10	4	2	2	15	20	20	27
15	Банки	21	7	53	0	11	1	4	2
100	Весь капітал	12	4	15	2	18	13	15	21
100	Весь капітал з очікуваним розподілом капіталу до визначення	12	4	16	3	21	21	23	

Джерело: (*Центр економічної стратегії, 2023*)

Так, у 2022 р. 300 найбільших підприємств України згенерували дохід у розмірі 142,0 млрд дол США, що становить приблизно 42 % від загального доходу всіх підприємств. Згідно з дослідженням, на іноземні компанії припадає близько 15% виручки 300 найбільших підприємств (у тому числі на корозійні структури – 5%). Частка публічного капіталу становить 23% (державний – 22%, комунальний – 1%), олігархічний капітал – 28%, а інший корозійний капітал – 6%. конструктивний капітал становить 12% від загального обсягу, і ще 16 % капіталу потенційно можна класифікувати як конструктивний або корозійний на основі додаткових даних дослідження компаній.

Загальна оцінна частка конструктивного капіталу в Україні становить не менше 15%. Ще 20% капіталу може бути конструктивним або корозійним за результатами більш глибоких досліджень, здебільшого - внутрішнім приватним конструктивним або внутрішнім приватним корозійним, рідше - іншими типами капіталу. Беручи до уваги очікуваний розподіл капіталу цієї категорії, загальна частка конструктивного капіталу в Україні може становити близько 22%. При цьому державні та комунальні компанії охоплюватимуть близько чверті сукупного капіталу, частка іноземного капіталу складатиме близько 17 %.

Високою є сукупна частка корозійного капіталу: 46%, який включає олігархічний капітал – 21%, іноземний – 5%, інший корозійний капітал – 20%. З урахуванням можливих похибок дослідження, частка конструктивного капіталу в Україні з високою ймовірністю коливається в межах 20- 25%.

Відповідно до статей 64 та 67 Бюджетного кодексу України, до місцевих бюджетів об'єднаних територіальних громад сплачуються податки, подані в таблиці 5.

Таблиця 5

Ресурси об’єднаних територіальних громад (ТГ)

Податки	60 % ПДФО;25 % екологічного податку;5 % акцизного податку з реалізації підакцизних товарів;100 % єдиного податку;100 % податку на прибуток підприємств комунальної власності; 100% податку на майно (нерухомість, земля, транспорт)
Збори та платежі	державне мито; плата за надання адміністративних послуг; збір за паркування; туристичний збір; орендна плата за користування майном у комунальній власності; рентні плати за користування надрами;50 % грошових стягнень за шкоду довкіллю;75 % коштів від відшкодування втрат сільськогосподарського і лісогосподарського виробництва; інше
Інші доходи	різноманітні трансферти (базова дотація, освітня і медична субвенції, капітальні трансферти) – найбільший інтерес для ТГ; цільові та добровільні внески установ до місцевих фондів охорони довкілля; надходження в рамках програм міжнародної технічної допомоги; кошти пайової участі у розвитку інфраструктури; кошти від відчуження комунального майна; кошти від реалізації безхазяйного майна; місцеві запозичення; інше

Джерело: складено автором за (*Бюджетний кодекс України, 2010*)

Як відзначає П. Сенищ, «…об’єднані територіальні громади перейшли на прямі міжбюджетні відносини з державним бюджетом і стали повноцінними суб’єктами бюджетного процесу. Така система прямого фінансування дозволила органам місцевого самоврядування отримувати такі міжбюджетні трансферти: базову дотацію; реверсну дотацію; освітню субвенцію; медичну субвенцію; інші субвенції, без зарахування цих коштів до районного чи обласного бюджетів» (*Сенищ П.М., Фугело П.М., 2022*).

На сьогодні, спостерігається значне скорочення дохідної частини місцевих бюджетів громад, на території яких ведуться бойові дії. Натомість в окремих областях помітне зростання за рахунок зростання чисельності військовозобов’язаних.

Розглянемо структуру місцевого бюджету Одеського регіону за 2023 р. (табл. 6).

Таблиця 6

Структура місцевого бюджету Одеського регіону за 2023 р.

Доходи			Видатки		
Статті доходів	млрд грн	Питома вага,%	Статті видатків	млрд грн	Питома вага,%
Податкові надходження	3717,98	51,36	Загальнодержавні функції	1821,71	29,98
Неподаткові надходження	424, 33	5,86	Громадський порядок, безпека, судова влада	32,29	0,53
Доходи від операцій з капіталом	1,79	0,02	Економічна діяльність	1165,99	19,19
Офіційні трансферти	3094,59	42,75	Охорона навколишнього природного середовища	31,42	0,52
Цільові фонди	0,84	0,01	Житлово-комунальне господарство	1,26	0,02
			Охорона здоров'я	484,94	7,98
			Духовний та фізичний розвиток	390,35	6,42
			Освіта	1609,68	26,50
			Соціальний захист та соціальне забезпечення	507,83	8,85

Джерело: (*Децентралізація, 2023*)

Як видно із представлених даних, серед доходів бюджету Одеського регіону у 2023 році складають податкові надходження (51,36 %); серед видатків – витрати, які покривають виконання загальнодержавних функцій (29,98 %).

Слід виокремити додаткові джерела наповнення бюджету територіальних громад, а саме: міжнародні програми фінансування проєктів на засадах співфінансування; міжнародні гранти, участь органів місцевого самоврядування в реалізації інвестиційних програм і проєктів на умовах співфінансування з державою; застосування механізму державно-приватного партнерства; продаж земельних ділянок або прав на них на конкурентних засадах.

На основі дослідження та аналізу нормативно-правових актів, що регулюють питання надання фінансової підтримки об'єднаним територіальним громадам в Україні можна виокремити інструменти фінансової підтримки територіальних громад.

У 2024 р. для підтримки органів місцевого самоврядування заплановано майже 24 млрд грн додаткової дотації з державного бюджету місцевим бюджетам для найбільш постраждалих прифронтових та фронтових територій. Базова дотація з державного бюджету місцевим бюджетам на наступний рік прогнозована у сумі 20,2 млрд грн (*Державний сайт України, 2024*).

У частині міжбюджетних трансфертів передбачено такі показники: збережено базову дотацію для 1014 бюджетів громад - це 18,8 млрд гри.; скасовано реверсну дотацію, в результаті чого для 235 громад збережено 12,4 млрд гри; 158,8 млрд грн на Програму медичних гарантій обслуговування населення; 103,2 млрд грн освітньої субвенції, з них 87,5 млрд грн розподіллено між бюджетами 1425 громад; 44,8 млрд грн. Резервного фонду; 33,4 млрд грн. додаткової дотації з державного бюджету місцевим бюджетам на здійснення повноважень органів місцевого самоврядування на деокупованих, тимчасово окупованих та інших територіях України, що зазнали негативного впливу у зв'язку з повномасштабною збройною агресією рф. 39 % такої дотації, тобто 13,1 млрд грн. дотації розподіллено між місцевими бюджетами, а саме: 9,7 млрд грн. між 418 бюджетами громад та 3,4 млрд грн. – між 6 обласними бюджетами Донецької, Запорізької, Луганської, Миколаївської, Харківської, Херсонської областей; 4,5 млрд грн. субвенції на проєкти в рамках Програми з відновлення України; 5,7 млрд гри. субвенцій на забезпечення житлом учасників бойових дій; 3,8 млрд грн. нової субвенції на забезпечення інституту помічника ветерана в системі переходу від військової служби до цивільного життя; 3,4 млрд грн. додаткових дотацій місцевим бюджетам, а саме на здійснення переданих з державного бюджетів видатків з утримання закладів освіти та охорони здоров'я, утримання соціальної інфраструктури, компенсування втрат доходів місцевих бюджетів від податкових пільг у галузі космічної діяльності та літакобудування; 2,5 млрд грн. субвенції на облаштування безпечних умов в школах; 2,3 млрд гри. субвенції на проєкти в рамках Надзвичайної кредитної програми для відновлення України; 1,7 млрд грн. субвенції на підтримку окремих закладів охорони здоров'я; 1,5 млрд грн. субвенції на програму «Нова українська школа»; 1,5 млрд грн. субвенції на придбавання обладнання, модернізацію їдальнь (харчоблоків); 1,0 млрд грн. субвенції на облаштування безпечних умов у закладах охорони здоров'я; 1,0 млрд грн. субвенції на придбання шкільних автобусів; 575,3 млн гривень субвенції на забезпечення житлом дітей-сиріт, дітей позбавлених батьківського піклування, осіб з їх числа; 500,0 млн грн. субвенції на створення навчально-практичних центрів сучасної професійної (професійно-технічної) освіти; 304,6 млн грн субвенції для підтримки осіб з особливими освітніми потребами; 248,4 млн грн. нової субвенції на реалізацію проєкту «Ремонт житла для відновлення прав і можливостей людей (HOPE)»; 200,2 млн грн. субвенції на створення служб з підтримки осіб, які постраждали від домашнього насильства; 54,0 млн грн. субвенції на реалізацію проєкту «Активні парки – локації здорової України»; 37,2 млн грн. субвенції на проєкт "Поліпшення охорони здоров'я на службі у людей»; 20,0 млн грн. субвенції на компенсацію ризику населенню у зоні спостереження (*Місцеві фінанси, 2024*).

Базова дотація є інструментом вирівнювання та підвищення фіскальної спроможності бюджетів об'єднаних територіальних громад. Вона надається бюджетам територіальних громад з загального фонду державного бюджету і джерелами перерахування цього трансферту є загальнодержавні податки і збори, що надходять до загального фонду державного бюджету (*Бюджетний кодекс України, 2010*). Базова дотація здійснюється на основі оцінки індексу податкоспроможності бюджету територіальної громади, якщо значення індексу менше 0,9, то надається базова дотація відповідному бюджету в обсязі 80 % суми, необхідної для досягнення індексом забезпеченості відповідного бюджету значення 0,9 (*Бюджетний кодекс України, ст. 99, 2010*).

Додаткові дотації з державного бюджету можуть надаватися бюджетам територіальних громад на компенсацію втрат доходів місцевих бюджетів, що не враховуються при визначенні обсягу міжбюджетних трансфертів, внаслідок наданих державою податкових пільг, які зменшують доходи цих місцевих бюджетів (*Бюджетний кодекс України, ст. 103, 2010*).

Освітня субвенція – це один з інструментів фінансової підтримки територіальних громад, обсяги якої для бюджетів територіальних громад окремо затверджуються у Законі України про Державний бюджет на поточний рік.

Освітня субвенція розподіляється між відповідними бюджетами на основі формули (*Постанова КМУ, 2017*) і спрямовується на оплату праці педагогічних працівників закладів освіти, що забезпечують здобуття повної загальної середньої освіти, зокрема: початкові школи, гімназії (крім дошкільних підрозділів у таких закладах), ліцеї; спеціальні школи; заклади спеціалізованої освіти: мистецькі, спортивні, військові (військово-морські, військово-спортивні), наукові ліцеї, ліцеї з посиленою військово-фізичною підготовкою; дитячі будинки, навчально-реабілітаційні центри, інклюзивно-ресурсні центри; заклади професійної (професійно-технічної) освіти державної та комунальної власності в частині забезпечення видатків на здобуття повної загальної середньої освіти; заклади фахової перед вищої освіти і коледжі державної та комунальної власності в частині забезпечення видатків на здобуття повної загальної середньої освіти *(Бюджетний кодекс України, ст. 103, 2010*).

Медична субвенція визначена Бюджетним кодексом України як трансферт, що надається з Державного бюджету України місцевим бюджетам, в тому числі бюджетам територіальних громад (*Бюджетний кодекс України, 2010)*. Обсяги медичної субвенції для бюджетів територіальних громад окремо затверджуються у Законі України про Державний бюджет на поточний рік (*Закон України, 2023*), та розподіляються між відповідними бюджетами на основі формули (*Постанова КМУ, 2015*).

Кошти медичної субвенції використовуються територіальними громадами для оплати поточних видатків на охорону здоров'я, крім видатків на оплату комунальних послуг та енергоносіїв, зокрема (*Бюджетний кодекс України, ст. 89, 2010*): амбулаторно-поліклінічну та стаціонарну допомогу (лікарні широкого профілю, спеціалізовані медико-санітарні частини, пологові будинки, поліклініки і амбулаторії, загальні стоматологічні поліклініки, дільничні лікарні); первинну медичну допомогу (медичні амбулаторії, фельдшерсько-акушерські і фельдшерські пункти, центри первинної медичної (медико-санітарної) допомоги та інші заклади охорони здоров'я, що надають первинну медичну допомогу); програми медико-санітарної освіти (центри здоров'я і заходи з санітарної освіти); інші державні програми медичної та санітарної допомоги (територіальні медичні об'єднання, центри медичної статистики, автопідприємства санітарного транспорту, інші програми і заходи); оплату комунальних послуг та енергоносіїв комунальними закладами охорони здоров'я, що надають первинну медичну допомогу, місцеві програми розвитку та підтримки комунальних закладів охорони здоров'я, що надають первинну медичну допомогу, та місцеві програми надання населенню медичних послуг з первинної медичної допомоги населенню; місцеві програми розвитку та підтримки комунальних закладів охорони здоров'я, які належать відповідним територіальним громадам, місцеві програми надання населенню медичних послуг понад обсяг, передбачений програмою державних гарантій медичного обслуговування населення; місцеві програми громадського здоров'я тощо.

Найпростішим для використання інструментом є інфраструктурна субвенція, яку отримують всі об'єднані територіальні громади на проекти, що відповідають плану соціально-економічного розвитку територіальних громад. Кошти розподіляються за формулою та напряму залежать від просторових чинників. Окрім відповідності плану соціально-економічного розвитку, умовами фінансування проєктів також є тривалість календарного плану реалізації проєкту не більше 3-х років, врахування потреб осіб з інвалідністю (*Демченко О.П., 2021*).

Інші субвенції визначаються можливостями Державного бюджету України та коригуються щорічно разом з прийняттям Закону України «Про Державний бюджет на поточний рік».

Якщо говорити про фінансову підтримку територіальних громад Одещини, то можна визначити основні канали інвестиційно-кредитного забезпечення (рис. 1).

Рис. 1. Система кредитно-інвестиційного забезпечення територіальних громад

Джерело: сформовано автором

1. Визначення фінансових можливостей регіонального ринку банківських послуг Одещини для стимулювання розвитку територіальних громад/

На сьогоднішній день, для фінансової підтримки розвитку Одеського регіону представляють інтерес три банки – ПАТ «МТБ Банк», АБ «Південний» та ПАТ «Банк Восток». При цьому слід зауважити, що «Банк Восток» за юридичною адресою не відноситься до Одеського регіону, але за розташуванням головного офісу у м. Одесі здійснює безпосередній вплив на формування регіонального ринку банківських послуг Одещини (*Коваленко В.В., Кулікова Є.О., 2022*).

При розгляді питання розвитку регіонального ринку банківських послуг Одещини, за необхідне є дослідження основних показників діяльності зазначених банків.

По-перше – це показники достатності їх капіталу. Розглянемо динаміку нормативу достатності зазначених банків під час воєнного стану в Україні (рис. 2).

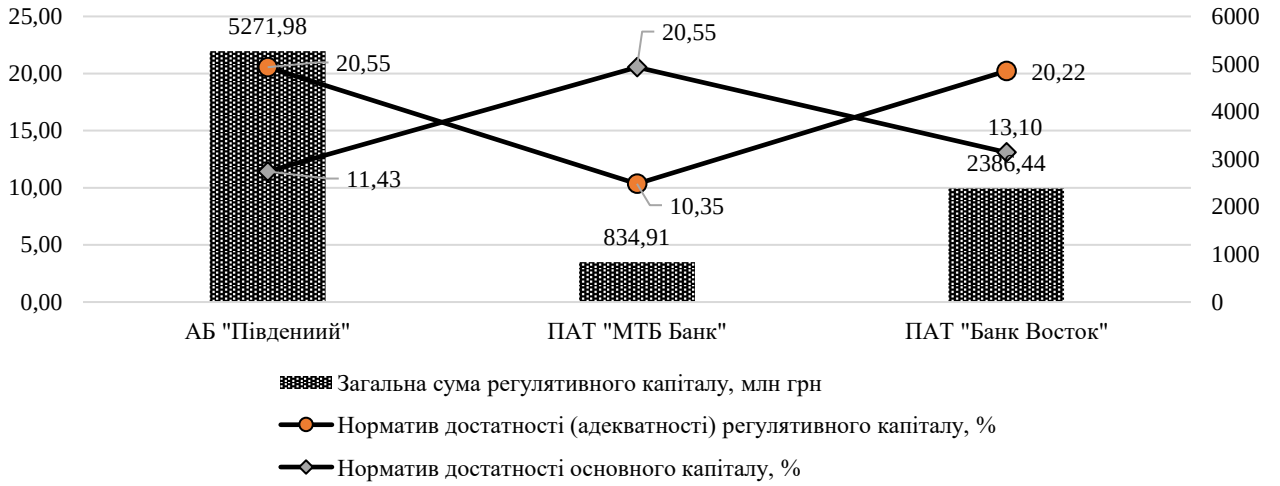


Рис. 2. Показники достатності капіталу АБ «Південний», ПАТ «МТБ Банк», ПАТ «Банк Восток» у 2023 році

Джерело: розраховано автором за матеріалами (*Національний банк України. Наглядова статистика, 2024*)

Як свідчать дані рисунку 2, банки, що аналізуються у повній мірі виконують нормативи достатності капіталу. Найбільш достатня капітальна база сформована АБ «Південний». Виконання нормативів капіталу банками, що аналізуються свідчить про те, що вони спромозі покривати ризики, які виникають під час їх діяльності, засвідчують їх платоспроможність.

По-друге – це показники прибутковості діяльності банків (рис. 3).

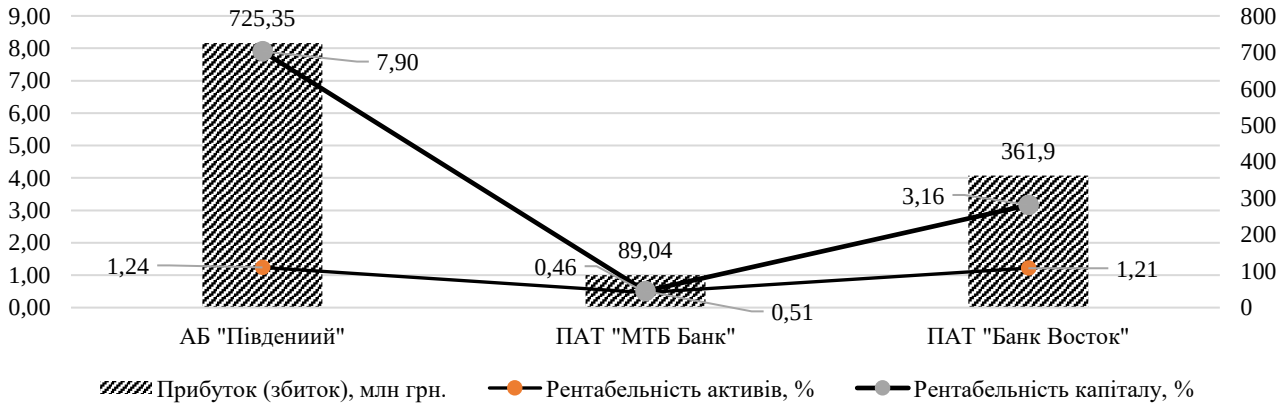


Рис. 3. Показники прибутковості діяльності АБ «Південний», ПАТ «МТБ Банк», ПАТ «Банк Восток» у 2023 році

Джерело: розраховано автором за матеріалами (*Національний банк України. Грошово-кредитна політика, 2024*)

Як видно із даних рисунку 3, лідером за рівнем прибутковості є АБ «Південний». Слід відзначити, що позитивним моментом є те, що за останнє десятиріччя дані банки не отримували збитку, що свідчить про виважену їх політику щодо управління активами та пасивами.

Як було зазначено вище, аналізовані банки в більшій мірі спричиняють вплив на розвиток ринку банківських послуг Одещини. Тому за доцільне, є дослідження їх кредитних та депозитних портфелів (табл. 7).

Таблиця 7

Динаміка депозитних портфелів ПАТ «МТБ Банк», АБ «Південний», ПАТ «Восток» за період 2019-2023 рр.

Суб'єкти	2019		2021		2022		2023*	
	млн грн.	Питома вага, %	млн грн.	Питома вага, %	млн грн.	Питома вага, %	млн грн.	Питома вага, %
ПАТ "МТБ Банк"								
К нфк	2267,49	50,28	6368,97	68,25	6342,79	66,97	12558,03	77,12
К д.г	2242,13	49,72	2963,48	31,75	3128,97	33,03	3725,95	22,88
Усього	4509,62	100,00	9332,45	100,00	9471,76	100,00	16283,98	100,00
ПАТ "Восток"								
К нфк	5686,33	63,95	12212,76	70,20	12134,95	71,22	19319,72	77,87
К д.г	3205,43	36,05	5184,14	29,80	4903,16	28,78	5490,13	22,13
Усього	8891,76	100,00	17396,9	100,00	17038,11	100,00	24809,85	100,00
АБ "Південний"								
К нфк	10410,01	53,11	24419,76	65,97	24413,33	68,15	27472,52	64,38
К д.г	9190,74	46,89	12595,23	34,03	11408,39	31,85	15200,88	35,62
Усього	19600,75	100,00	37014,99	100,00	35821,72	100,00	42673,4	100,00

К нфк – Кошти не фінансових корпорацій; К д.г- Кошти домашніх домогосподарств

Джерело: розраховано автором за матеріалами (*Національний банк України. Наглядова статистика, 2024*)

Як свідчать дані таблиці 7, депозитний портфель банків, що аналізуються, характеризується тим, що на протязі досліджуємого періоду спостерігається тенденція щодо урівноваження залучених коштів від нефінансових корпорацій та домашніх домогосподарств. Так, у ПАТ "МТБ Банк" в 2019 р. зазначене співвідношення практично було урівноважено за питимою вагою по 50 %. У 2022 р. та 2023 р. переважають кошти нефінансових корпорацій, які склали 66,97 % та 77,02 % відповідно.

У АБ "Південний" та ПАТ "Восток" також переважають у структурі кошти залучені від нефінансових корпорацій. Хоча, АБ "Південний" у 2023 р. збільшив портфель коштів

домогосподарств у порівнянні з 2022 р. на 12,5 %, надивлячись на складну ситуацію в країні, це свідчить про довіру населення до банку.

Найбільший депозитний портфель як в цілому, так і за суб'єктами залучення коштів у АБ "Південний" на протязі досліджуємого періоду.

Далі розглянемо динаміку кредитних портфелів банків, що аналізуються (табл. 8).

Таблиця 8

Динаміка кредитних портфелів ПАТ «МТБ Банк», АБ «Південний», ПАТ «Восток» за період 2019-2023 рр.

Суб'єкти кредитування	2019		2021		2022		2023	
	млн грн.	Питома вага, %	млн грн.	Питома вага, %	млн грн.	Питома вага, %	млн грн.	Питома вага, %
ПАТ "МТБ Банк"								
К нфк	2173	91,07	4078,06	93,47	3957,3	93,47	15928,17	99,72
К д.г	212,92	8,93	284,81	6,53	210,69	6,53	45,5	0,28
Усього	2 385	100,00	4362,87	100,00	4167,99	100,00	15973,67	100,00
ПАТ "Восток"								
К нфк	6603,65	98,48	9042,12	98,93	8157,41	98,93	8569,31	98,39
К д.г	101,85	1,52	98,05	1,07	89,64	1,07	140,02	1,61
Усього	6705,5	100,00	9140,17	100,00	8247,05	100,00	8709,33	100,00
АБ "Південний"								
К нфк	12906,49	98,83	19822,71	99,27	15580,91	99,27	15928,17	99,72
К д.г	152,62	1,17	146,35	0,73	719,23	0,73	45,5	0,28
Усього	13059,11	100,00	19969,06	100,00	16300,14	100,00	15973,67	100,00

К нфк – Кошти не фінансових корпорацій; К д.г- Кошти домашніх домогосподарств

Джерело: складено автором за матеріалами (*Національний банк України. Наглядова статистика, 2024*)

Як свідчать дані таблиці 8 кредитні портфелі банків, що аналізуються, спрямовані на суб'єктів нефінансових корпорацій. Про це свідчить їх питома вага в структурі кредитного портфеля. Так, в 2023 р. у ПАТ «МТБ Банк» вона склала – 99,72 %, ПАТ «Банк Восток» – 98,39 %, АБ «Південний» – 99,72 %.

Якщо розглядати зміну кредитних портфелів у абсолютному значенні, то слід відзначити, що за період 2019-2023 рр. спостерігається їх зростання, а саме: ПАТ «МТБ Банк» на 13 755 млн грн. в 2023 р. у порівнянні з 2019 р.; у

ПАТ «Восток» на 1965,66 млн грн.; у АБ «Південний» на 3021,68 млн грн. відповідно.

Найбільший кредитний портфель як в цілому, так і за суб'єктами кредитування, спостерігається у АБ «Південний» на протязі досліджуємого періоду.

У подальшому, слід визначитися зі ступенем ефективності обслуговування банками клієнтів за допомогою показників чистої процентної маржі, середньої вартості залучення ресурсів, середньої ціни надання кредитних продуктів та прибутковості/ збитковості продаж (табл. 9).

Таблиця 9

Динаміка показників чистої процентної маржі, середньої вартості залучення ресурсів, середньої ціни надання кредитних продуктів та прибутковості/ збитковості продаж ПАТ «МТБ Банк», АБ «Південний», ПАТ «Восток» за період 2017-2023* рр.

Роки	Середня ціна надання кредитних продуктів	Середня вартість залучення ресурсів	Чистий спред	Чиста процентна маржа	прибутковості/ збитковості продаж, %
ПАТ "МТБ Банк"					
2017	19,03	3,93	3,07	15,10	1,62
2018	21,48	3,74	17,74	4,96	0,40
2019	21,86	5,16	16,70	5,10	1,10
2020	18,94	3,58	15,36	4,25	1,13
2021	20,48	3,63	16,85	4,40	1,22
2022	17,01	5,04	11,97	2,79	0,07
2023	26,41	5,77	20,64	2,00	0,46
ПАТ "Восток"					
2017	15,27	5,81	5,73	9,47	0,95
2018	14,69	6,07	8,62	5,92	1,26
2019	17,31	5,68	11,62	5,93	1,49
2020	15,78	3,29	12,48	4,06	0,90
2021	15,01	2,47	12,54	4,75	1,44
2022	14,01	2,77	11,24	4,09	0,84
2023	30,53	10,72	19,81	8,92	1,21
АБ "Південний"					
2017	13,54	15,94	-2,4	2,42	0,3
2018	12,73	8,32	4,41	1,31	1,02
2019	14,94	8,37	6,57	1,05	1,07
2020	19,87	8,50	11,37	3,40	0,73
2021	15,39	3,39	12,00	3,71	1,42
2022	14,19	4,17	10,02	3,92	0,83
2023	37,94	7,61	30,33	4,81	1,24

Джерело: складено автором за матеріалами *(Національний банк України. Наглядова статистика, 2024)*

Як свідчать представлені дані у таблиці 9, основні показники, які характеризують рівень ефективності обслуговування клієнтської бази ПАТ «МТБ Банк», ПАТ «Восток» та

АБ «Південний», знаходяться на достатньому рівні. Це означає, що стратегія управління у банку є виваженою. Виключенням є 2017 рік, коли АБ «Південний» вдавався до агресивної політики щодо залучення ресурсів, і тим самим чистий спред був отриманий від'ємний.

У подальшому слід розглянути загальні тенденції розвитку ринку банківських послуг в Одеському регіоні. Розглянемо основні показники грошово-кредитної та фінансової статистики діяльності депозитних корпорацій (банків) Одеської області станом на кінець грудня 2023 р. Даний період обраний виходячи з того, що воєнні події, які відбуваються на території Одеської області вимагають додаткової фінансової підтримки для відновлення критичної інфраструктури та відбудови постраждалих громад.(табл. 10).

Таблиця 10

Надані кредити та залучені депозити банками Одещини на кінець 2023 р.

Показники	Залишки коштів, млн грн			Зміна, %		
	Україна	Одеська область	% до загального підсумку по Україні	у річному обчисленні	до початку року	за місяць
Кредити, надані депозитними корпораціями						
Нефінансовим корпораціям:	735 295	28 235	3,8	–1,1	–1,1	1,5
у національній валюті	495 414	19 748	4,0	7,1	7,1	–0,0
у іноземній валюті	239 881	8 486	3,5	–16,0	–16,0	5,1
Домашнім домогосподарствам	236 470	9 672	4,1	–1,1	–1,1	–1,6
у національній валюті	224 043	8 576	3,8	–0,8	–0,8	–2,2
у іноземній валюті	12 427	1 096	8,8	–3,5	–3,5	3,1
Депозити, залучені на рахунки						
Нефінансовим корпораціям:	1031122	44 728	4,3	13,0	13,0	10,0
у національній валюті	754 041	27 580	3,7	21,9	21,9	12,6
у іноземній валюті	277 081	17 149	6,2	1,2	1,2	6,2
Домашнім домогосподарствам	1228 46	58 848	4,8	13,0	13,0	4,1
у національній валюті	795 493	30 770	3,9	19,9	19,9	4,9
у іноземній валюті	433 053	28 078	6,5	6,3	6,3	3,2

Джерело: складено автором за матеріалами (*Національний банк України. Грошово-кредитна політика, 2024*)

Як свідчать дані таблиці 10, кредити, надані депозитними корпораціями Одещини у грудні місяці 2023 р. склали нефінансовим корпораціям 3,8 %, домашнім

домогосподарствам 4,1 % від загального обсягу по Україні. Депозити, залучені на рахунки відповідно склали від нефінансових корпораціям 4,3 %, домашнім домогосподарствам 4,8 % від загального обсягу по Україні. При дослідженні середньозважених процентних ставок за залученими та розміщеними коштами банками Одещини можна констатувати, що вони не відрізняються від середніх по Україні, а у деяких випадках і вищі.

2. Теоретико-методичне підгрунтя створення фінансових кластерів для забезпечення розвитку територіальних громад

Формування фінансових кластерів пов’язане з детермінантами національної конкурентоспроможності й є проявом їх системності. кластерна форма організації на основі мережі стійких зв’язків між усіма членами кластера є особливою формою ефективної трансформації знань в інновації, а інновацій – у конкурентні переваги. Кластеризацію в сучасній світовій економіці фахівці багатьох країн розглядають як елемент сталого економічного зростання та способу підвищення конкурентоспроможності. Кластери виконують роль «точок зростання», які здатні сформувати фундамент для динамічного економічного розвитку країни (*Зарічна Н.З., 2021*).

Кластер – це галузеве, територіальне та добровільне об'єднання організацій, які тісно співпрацюють між собою, а також з іншими суб’єктами в ланцюжку створення цінності з метою підвищення конкурентоздатності власної продукції, її експорту й сприяння економічному розвитку регіону (*Національна програма кластерного розвитку до 2027, 2020*).

В Україні налічується близько 30 створених кластерів (рис. 4). Але, єдиної організації – репрезентанта кластерів України немає, так само як немає кластерних

державних програм.

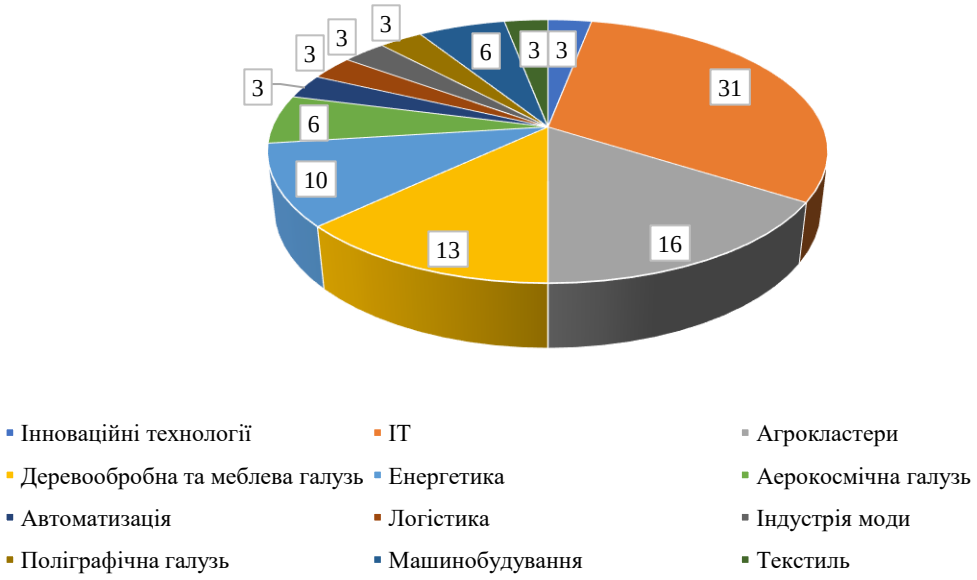


Рис. 4. Розподіл кластерів України за видами економічної діяльності

Джерело: (*Національна програма кластерного розвитку до 2027, 2020*)

Однією з перших країн Центральної та Східної Європи, де починаючи з 2000-х національний уряд підтримував розвиток корпоративного співробітництва та кластерів, була Угорщина. Саме в цій країні за ініціативи урядової програми в 2001 р. був створений перший в центрально-східній Європі кластер –PANAC: (Pannon Automotive Cluster) (*Evropian Claster Collaboration Platform, 2024*). Після приєднання до ЄС в 2004 р. кластерна політика отримала можливість впровадження додаткових інструментів підтримки, поділивши кластерні організації на 3 рівні –стартапи, регіональні та акредитовані.

У 2014 р. проведені дослідження кластерного розвитку в країні засвідчили, що з 176 стартапів тільки третина змогла успішно використати грантове фінансування та перерости в акредитовані кластери, що на сьогодні мають найбільший вплив на економічний розвиток Угорщини, зокрема в галузі науково-дослідних розробок. Тому, була створена спеціальна урядова комісія, яка проводить моніторинг та акредитацію кластерів, визначаючи пріоритетні інструменти підтримки.

Таку модель частково запозичив уряд Польщі, провівши в 2018 р. конкурсний відбір ключових національних кластерів та надавши їм пріоритет в доступі до грантових проєктів (*Ministry of Development and Technology, 2024*). Чехія, Румунія та Словаччина, які останніми з країн Східної Європи на початку 2020 р. запровадили програму підтримки та розвитку акредитованих кластерів (*Evropian Claster Collaboration Platform, 2024*). Литва та Латвія зробили пріоритезацію на смарт спеціалізації та експортний потенціал, в чому підтримують

кластери. Слід звернути увагу на те, що у всіх країнах існують кластерні асоціації, які виконують представницьку функцію, а також напряму співпрацюють з урядом при створенні стратегічних документів та програм.

Україна незважаючи на досить високу активність створених кластерів як на місцевому, національному так і на міжнародному рівні (зокрема, участь в Європейській спільноті кластерів – European Clester collaboration platform), кооперація з європейськими кластерами в обміні досвідом, кращими практиками та спільних транскордонних проєктах) значно відстає в напрямку імплементації державної політики та стратегії.

Для ефективності кластерної політики вона перш за все повинна бути простою - в операційному менеджменті, звітування та взаємодії з урядовими організаціями; передбачуваною - стейкхолдери можуть бути певними стабільності умов, фінансування та управлінських принципів; прозорою - усі сторони мають однаковий доступ до тієї самої інформації; забезпечувати фінансування - довготермінове фінансування протягом 5–10 років; далекостратегічною - перспектива 10–20 років.; узгодженою - з ключовими національними політиками, стратегіями та програмами; розробленою за участі всіх сторін -представниками індустрії, уряду, бізнесом, інвесторами та освітньо-наукового кола; розробленою для розвитку можливостей та компетенцій -включати програми тренінгів та навчань кластерного розвитку та управління (*Evropian Claster Collaboration Platform, 2024*).

Кластерні проєкти та ініціативи оптимізують взаємозв'язок між видами діяльності, механізмами, сервісами, інструментами та ресурсами й направляють їх на виконання тих чи інших цілей (рис. 5).

Рис. 5. Механізми впливу державної політики на кластерний розвиток та його результати

Джерело: сформовано автором

Таким, чином інструменти є складовими механізмів, які обслуговують ті чи інші види діяльності. Не зважаючи на довгий період існування, кластерний рух в Україні є слабо організованим на національному рівні. Кластерний розвиток слабо підтримується державою, та до 2020 р. були відсутні державні органи управління, відповідних національних політик чи програм розвитку.

Головні орієнтири та завдання кластерного розвитку відповідно до «Національної програми кластерного розвитку до 2027 року» представлено у таблиці 11.

Таблиця 11

Орієнтири та завдання кластерного розвитку в Україні

Цілі розвитку	2021	2024	2027
Інституціоналізація розвитку кластерів			
Введення державного реєстру, початкова атестація. Кількість атестованих кластерів в реєстрі.	20	30	45
Підтримка на центральному та регіональному рівнях (державні фонди), кількість кластерів, що фінансово підтримуються державою	5	10	25
Підтримка міжнародними фондами	7	10	15
Зростання вкладу кластерів в показники економічного розвитку регіонів та галузей			
Вклад кластерів в ВВП регіонів (середньостатистична оцінка по групі зареєстрованих кластерів)	TBD	+5 %	+6%
Кількість робочих місць	TBD	+7%	+10%
Кількість кластерів, які мають власну цифрову програм	TBD	+20%	+30%
Обсяги залучених інвестицій, грн	TBD	+10%	+20%
Інтернаціоналізація кластерів(експорт, міжнародна співпраця, інтеграція в глобальні ланцюги доданої вартості)			
Доля кластерів в регіональному експорті (за визначеними регіонами)	TBD	+8%	+15%
Кількість діючих міжнародних угод за участю українських кластерів	TBD	+10%	+15%
Кількість проєктів ЄС, в яких приймають участь українські кластери	TBD	+15%	+20%

*TBD – було заплановано для визначення пізніше

Джерело: (*Національна програма кластерного розвитку до 2027, 2020*)

Попри усі намагання, ініціативних угрупувань, дана концепція не набула законодавчо-утворюваного вигляду. Але, закладені у неї норми, правила та інструменти мають подальший розвиток, попри усі обставини, які супроводжують соціально-економічний розвиток в Україні.

Слід відзначити, що на відміну від традиційної форми організації бізнесу, функціонування кластерів має свою специфіку. Кластери об’єктивно існують, через них проходять значні грошові потоки. Доступні інструменти фінансового забезпечення для створення кластеру представлено на рисунку 6.

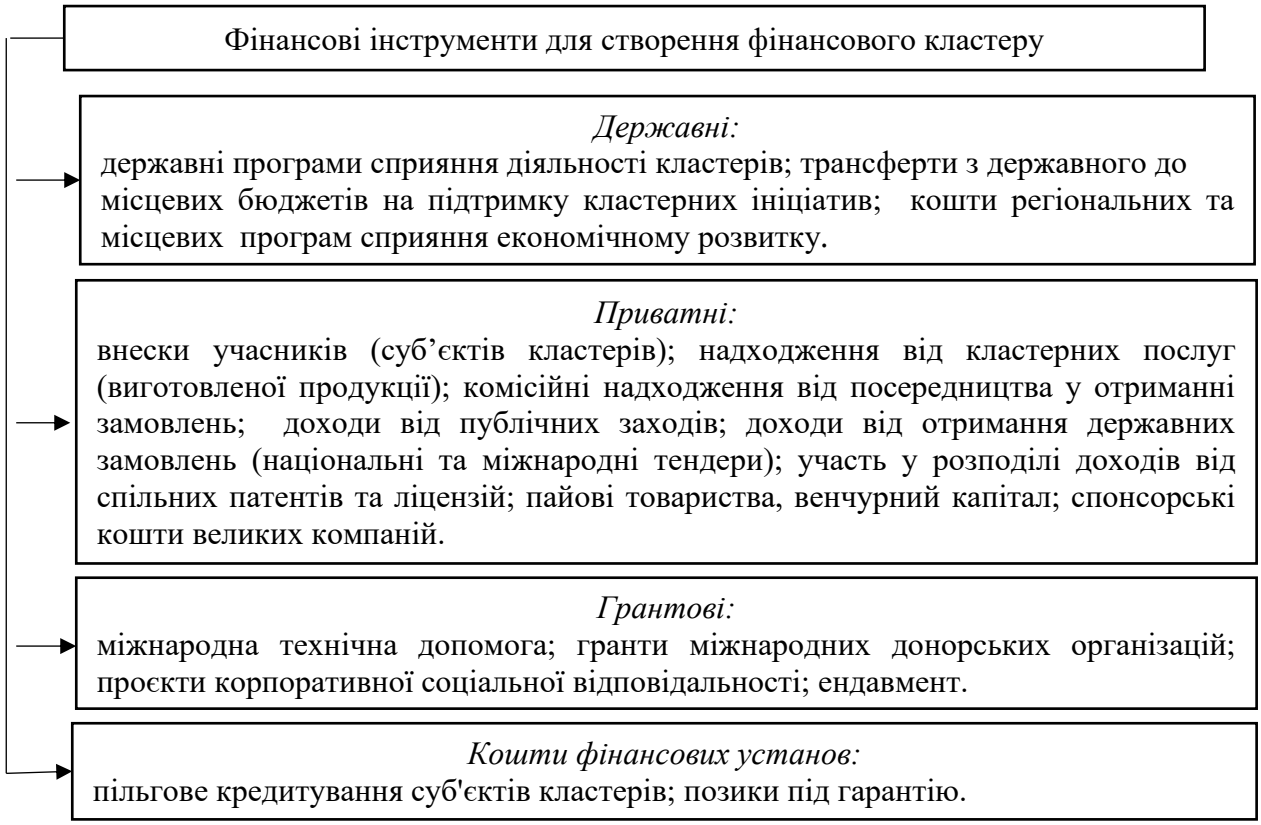


Рис. 6. Інструменти фінансового забезпечення функціонування кластерних угрупувань

Джерело: сформовано автором

Для створення фінансового кластеру, обсяг фінансового потенціалу визначається на етапі створення інтегрованої структура бізнесу (*Щербак В. Г., Готра В.В., 2016*). Функціонування кластерних утворень і оптимальне величина фінансового потенціалу визначається якісно і кількісно в залежності від складу кластера, його структури та потенційного проєкту. Основні завдання концепції управління фінансовим потенціалом кластерного об'єднання є наступні елементи (рис. 7).

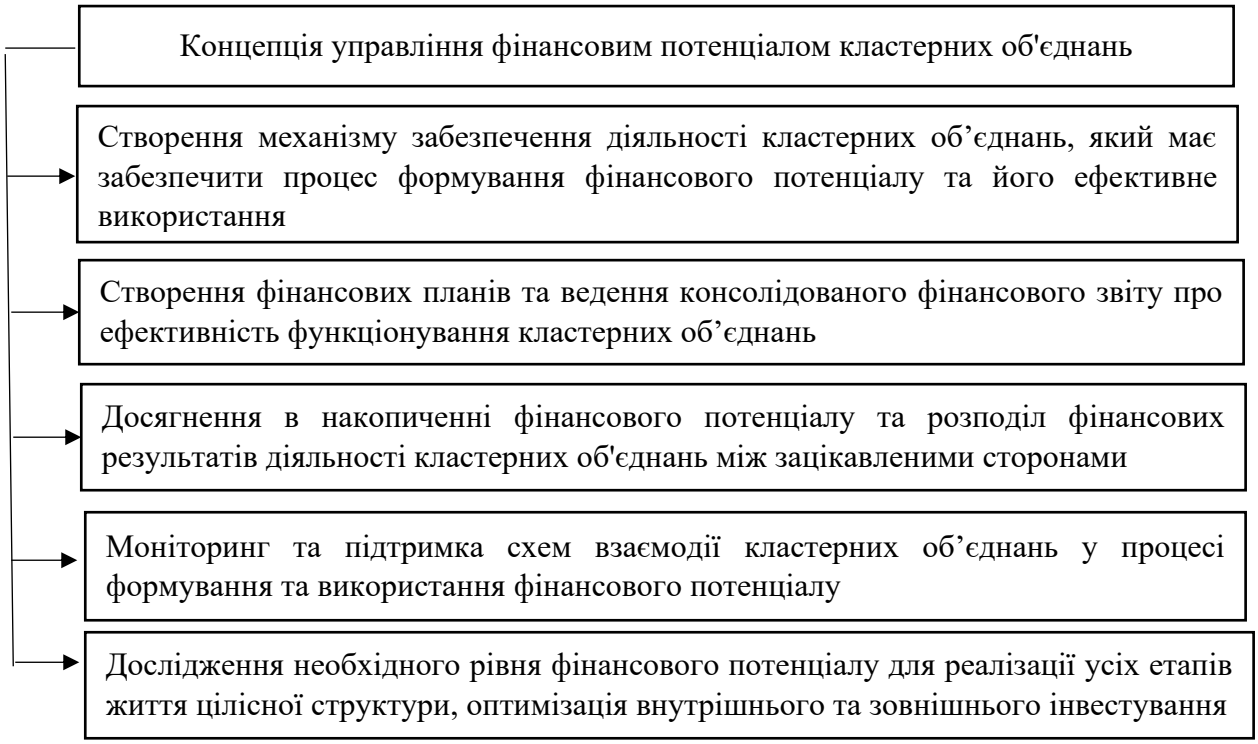


Рис. 7. Основні завдання концепції менеджменту фінансового потенціалу кластерних об'єднань

Джерело: сформовано автором з використанням джерел (*Пузирьова П., 2019; Ганущак-Єфіменко Л. М. , 2015*).

Ефективне функціонування системи управління фінансовим потенціалом кластерних об’єднань можливі за умови дотримання наступних принципів:

✓ інтеграція в загальну систему управління кластером, яка забезпечує узгодження управлінських рішень в процесі формування та використання фінансового потенціалу кластера з планами, діяльністю та управлінськими рішеннями;

✓ ефективність системи управління фінансовим потенціалом кластерних об’єднань, що передбачає наукове обґрунтування управлінських рішень, об’єктивну їх оцінку та результатів їх реалізації;

✓ адаптація системи управління фінансами потенціал кластерних об'єднань відповідно до структури об'єднання та чинників, що її визначають;

✓ орієнтація на стратегічні цілі розвитку. яка передбачає прийняття управлінських рішень, які повинні бути орієнтовані на стратегічні цілі розвитку інтегрованої структури та враховують можливості, а також зацікавленість кластерних об'єднань.

Для створення кластерів на певній території за необхідне провести дослідження щодо кон’юнктури ринку в першу чергу - фінансового та ресурсного потенціалу, аналізу

діяльності економічних суб'єктів, рівня фінансової обізнаності та інклюзії населення, а також інфраструктурного забезпечення.

Н. Зарічна виокремлює шість етапів створення кластерів, а саме:

1. Формування кластера може бути зумовлене історичними обставинами, такими як інтенсифікація ресурсів (фінансових, природних, трудових, виробничих); високий рівень знань у науково-дослідних організаціях; географічна концентрація фірм, установ, а також клієнтів; розташування підприємств, компаній, що продукують інновації в технологіях, котрі стимулюють зростання інших суб'єктів підприємництва.

2. Коли установи агломеруються, вони починають отримувати додаткові вигоди від мережевої взаємодії, зумовленої зовнішніми чинниками, й акумулюють її. Першим зовнішнім економічним чинником є створення групи спеціалізованих інфраструктурних установ, які часто утворюються після вертикальної дезінтеграції компаній та створення спеціалізованого ринку праці.

3. Формування нових організацій (установ), що надають послуги кільком фірмам (територіальним громадам) у зростаючому кластері (науково-дослідні інститути, бізнес-асоціації, бізнес-інкубатори).

4. Розвиток кластера і виникнення нових бізнес структур збільшують привабливість мережі для економічних суб'єктів країни та створюється бренд території, що сприяє збільшенню кількості членів кластера та їхніх клієнтів.

5. Формування тісних відносин між учасниками мережі сприяє безкоштовному обміну інформацією, знаннями, досвідом.

6. Кластер може бути успішним десятки років або ж стати частиною нового мережевого об'єднання (*Зарічна Н.З., 2021*).

Як відзначено у посібнику з кластерного розвитку, у рамках проєкту ЄС «Послуги підтримки МСП в пріоритетних регіонах», «…багато кластерів раніше чи пізніше потрапляють у стадію занепаду через те, що бізнес-поведінка у технологічному, інституціональному, соціальному та/або культурному аспектах стає більш внутрішньо орієнтованою» (*Посібник з кластерного розвитку, 2006*).

Доцільно виокремити основні стимулюючі фінансово-економічні чинники, які спонукають фінансово-кредитні інститути, органи влади, представників громади та бізнесу до мережевої взаємодії, а саме: формування стабільної та ефективної системи бізнес-процесів; світові фінансові кризи; інвестиційна неспроможність; податкове навантаження; глобалізація економік; залучення додаткових фінансових ресурсів; економіка знань; конкуренція та інше.

З метою забезпечення ефективного функціонування фінансових кластерів за необхідне є використання системного підходу, який передбачає формування механізму управління їхньою діяльністю (рис. 8).

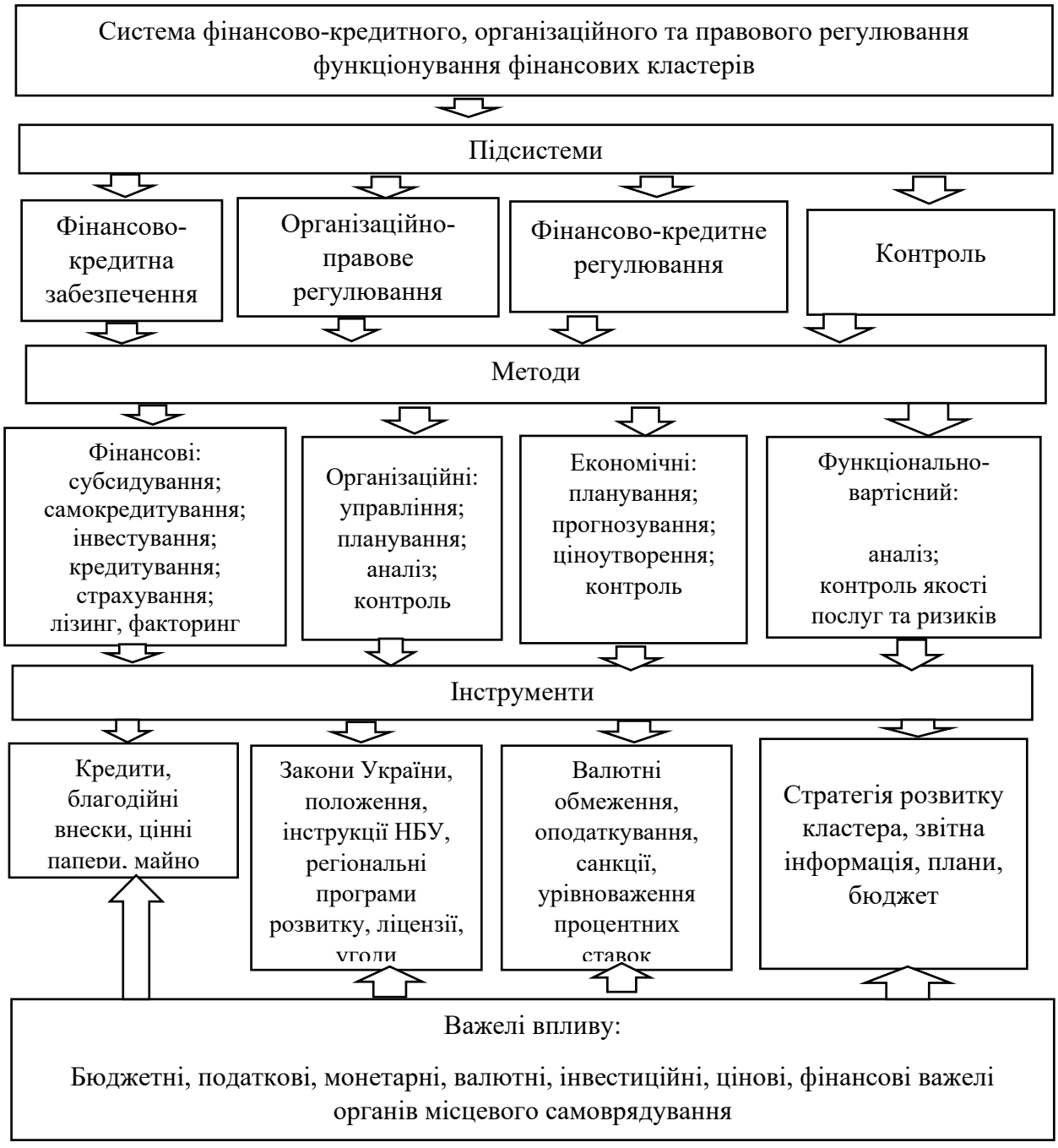


Рис. 8 Система фінансово-кредитного, організаційного та правового регулювання функціонування фінансових кластерів

Джерело: сформовано автором

З нашої точки зору, саме банки повинні бути ініціатором створення таких фінансових кластерів. В інтегрованих структурах кластерного типу поширеною формою кредитування

є взаємне кредитування, що передбачає фінансування операції/ проєкту одного з учасників об'єднання з кредитів, наданих іншими учасниками кластеру. Таке джерело формування фінансового капіталу інтегрованого об'єднання виступає ефективним інструментом оперативного фінансування членів кластеру.

На сьогодні, за участю банківських угрупувань у кластери з поєднанням з територіальними громадами, набуває актуальності реалізація програм «зеленого банкінгу». Так, Л. Кучер та співавтори довели, що «…зелений банкінг реалізується двосторонньо: по-перше, як механізм банківського менеджменту, спрямований на зменшення шкоди довкіллю та витрат унаслідок поточної операційної діяльності банків (внутрішній або власний «зелений» банкінг), а по-друге, як механізм надання грошових кредитних ресурсів для стимулювання екологічних проєктів, виробництва «зелених» технологій, екологічних товарів і послуг або для розвитку діяльності зі збереження довкілля» (Кучер Л.Ю., Кучер А.В. та Тріпілець О.В., 2020).Саме другий вид механізму реалізації зеленого банкінгу є складовою частиною економічного механізму екологічного регулювання як потенційний новий механізм вітчизняної екологічної політики і привертає найбільшу увагу як складник «зелених» фінансів» для створення фінансових кластерів.

Прикладом такого банку є державний банк АТ «Укргазбанк», який обрав стратегії реалізації «зеленого банкінгу», яка ґрунтується на таких основних постулатах як:

- ✓ спеціальні відсоткові ставки за еко-кредитами;
- ✓ унікальна методика, розроблена банком у співпраці з Міжнародною фінансовою корпорацією (IFC), допомагає реалістично оцінити очікувані результати на етапі попереднього розгляду. Це дозволяє за потреби коригувати проєкт для досягнення оптимальних показників окупності та економії енергозатрат;
- ✓ проста й швидка процедура оформлення кредиту;
- ✓ гарантії надійності державного банку;
- ✓ співпраця з акредитованими партнерами дозволяє прискорити узгодження проєкту, таких як LED освітлення; котельне обладнання; енергоефективне обладнання, енергозберігаючі вікна, двері; транспортні засоби; утилізація відходів; еко-партнер-генеральний підрядник; енергоаудит; медична техніка та обладнання (*Офіційний сайт АТ «Укргазбанк», 2024*).

Даний напрям можливо узяти за основу створення фінансового кластеру для підтримки територіальних громад Одеського регіону на базі банків-юридичних осіб, які працюють на території Одещини.

Ефективність використання даних форм можлива за допомогою створення фінансового кластеру у регіоні.

Висновки.

На сучасному етапі розвитку економіки України актуалізується питання щодо нейтралізації диспропорцій у розвитку регіональних ринків банківських послуг, які викликані наявністю на території банків - юридичних осіб, станом економічного розвитку регіону та фінансовими можливостями для стабільного функціонування територіальних громад.

Стабільне функціонування регіональних ринків банківських послуг ускладняються введенням воєнного стану в Україні, подовженням сплесків пандемії COVID 19, значними руйнуваннями у громадах та критичної інфраструктури. Все це вимагає пошуку альтернативних джерел фінансування для відновлення територій, пошуку дієвих механізмів інвестиційної підтримки соціально-економічного розвитку регіонів. Тому, за потрібне оцінити можливості регіонального ринку банківських послуг щодо формування фінансового кластеру для визначення стратегічних напрямів відновлення та подальшого розвитку територіальних громад.

У роботі надано характеристику каналів фінансової підтримки розвитку територіальних громад на підставі формування системи інвестиційно-кредитного забезпечення, яка являє собою сукупність економічних відносин, що виникають з приводу пошуку різних джерел фінансових ресурсів, їх залучення і ефективного використання та організаційно-управлінських принципів, методів, форм для впливу на соціально-економічну діяльність територіальних громад.

До основних форм інвестиційно-кредитного забезпечення розвитку територіальних громад віднесено: державна підтримка, банківське кредитування та інвестування.

Доведено, що реалізація запропонованих форм інвестиційно-кредитного забезпечення вимагають впершу чергу розробки певних напрямів щодо фінансової підтримки, яка акумулюється на регіональних ринках банківських послуг. Під час аналізу регіонального ринку банківських послуг Одещини доведено, що такі банки як ПАТ «МТБ Банк», АБ «Південний» та ПАТ «Банк Восток» можуть бути основою для створення фінансового кластеру щодо підтримки територіальних громад Одещини.

Сформовано систему фінансово-кредитного, організаційного та правового регулювання функціонування фінансових кластерів, яка додатково вимагає таких важелів впливу як бюджетних, податкових, монетарних, валютних, інвестиційних, цінових, фінансових важелів органів місцевого самоврядування.

Таким чином можна підвести підсумок. Банки Одещини на сьогодні функціонують у складних соціально-економічних та політичних умовах, спричиненими воєнною агресію рф. При цьому слід відміти, що незважаючи на це вони зберігають свої конкурентні позиції, основний вектор якої є підтримка соціально-економічного розвитку регіону та розвиток ринку банківських послуг Одещини.

Подальшого дослідження потребують питання, які пов'язані з новими формами фінансово-інвестиційний підтримки розвитку територіальних громад, а саме: розробка програм консорціумного кредитування; розширення довгострокового та інвестиційного кредитування шляхом запровадження механізмів проєктного фінансування як безрегресного методу фінансування, який інвестує проєкти, заснованих на прогнозованих грошових потоках; розробка концепції державного стимулювання банківського кредитування зруйнованих та пошкоджених територій (громад) та подальшого їх інноваційного розвитку; механізмів інституціонально-інфраструктурної підтримки в системі державно-приватного партнерства, застосування якого дозволяє впливати та забезпечувати збалансований розвиток територій.

References:

Герасимчук З.В., Гоманюк О.К. Фактори впливу на розвиток регіональних ринків банківських послуг. *Фінансовий простір*. 2015. № 1 (17). С. 92-101.

Гасій О. В., Соколова А.М., Прохар Н. В. Фактори конкурентного середовища банківському секторові економіки: регіональний аспект. *Ефективна економіка*. 2021. № 5. DOI: 10.32702/2307-2105-2021.5.85.

Чала В. С. Особливості фінансових інструментів зеленого банківництва на світовому ринку банківських послуг. *Економічний простір*. 2021. № 176. С. 28-36. DOI: https://doi.org/10.32782/2224-6282/176-4.

Мураєв Є. Розробка стратегії розумних міст України за збалансованою системою показників в умовах цифрової економіки. *Вісник Хмельницького національного університету*. .2020. № 4. Т. 2. С. 106-109. DOI: 10.31891/2307-5740-2020-284-4(2)-18.

Польова О. Децентралізація у забезпеченні стійкого економічного та соціального розвитку територіальних громад. *Економіка та суспільство*. 2022. Вип. 37. DOI: https://doi.org/10.32782/2524-0072/2022-37-53.

Ажажа М., Фурсін О., Венгер О. Зарубіжний досвід регіонального економічного розвитку: інновації, екосистема, місцеве самоврядування. *Humanities Studies*. 2022. Вип. 11 (88). С. 169-182.

Содома Р., Дубневич Ю., Марків Г., Шматковська Т.. Моніториг соціально-економічного розвитку територіальних громад. *Вісник Львівського національного аграрного університету. Економіка АПК*. 2021. №28. С. 24-30 DOI: https://doi.org/10.31734/economics2021.28.024.

Зарічна Н.З. Механізм фінансово-економічного забезпечення функціонування фінансових кластерів. *Східна Європа: економіка, бізнес та управління.* 2021. Вип. 4 (31). С. 106-111. DOI: https://doi.org/10.32782/easterneurope.31-17.

Puzyrova P. Concept of management and formation of financial potential of cluster unions. *Management*. 2019. Issue 1 (29). P. 109-119. DOI: 10.30857/2415-3206.2019.1.9.
Popelo O., Butko M., Revko A., Garafonova O., Rasskazov O. Strategy of the formation and development of an innovation agroindustrial cluster of the region in a context of decentralization of the authoritative powers. *Financial and credit activity: problems of theory and practice.* 2021. № 2 (37). P. 219-230. URL: https://fkd.net.ua/index.php/fkd/article/view/3309/3194.
Децентралізація (2024). Уряд Великої Британії надасть підтримку 10 територіальним громадам у відновленні. URL: https://decentralization.gov.ua/news/17618.
Децентралізація (2023). Міжнародна підтримка. URL: https://decentralization.gov.ua/donors.
Центр розвитку «Час змін». Місцеве самоврядування. URL: https://chaszmin.com.ua/category/mistseve-samovryaduvannya/.
Центр економічної стратегії. Конструктивний капітал в Україні. URL: https://ces.org.ua/research-constructive-capital-in-ukraine/.
Бюджетний кодекс України: Закон України, прийнятий Верховною радою України від 08.07.2010 р. № 2456-VI (із змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/2456-17#Text.
Сеницщ П.М., Фугело П.М. Фінансово-бюджетна підтримка соціально-економічного розвитку територіальних громад в умовах війни. Економіка та суспільство. 2022. Вип. 39. DOI: https://doi.org/10.32782/2524-0072/2022-39-89.
Державний сайт України. Бюджет-2024: у Мінфіні обговорили основні показники бюджету із асоціаціями органів місцевого самоврядування та облдержадміністраціями. URL: http://surl.li/qwfue.
Місцеві фінанси. Держбюджет на 2024 рік ухвалено. URL: https://auc.org.ua/novyna/derzhbyudzhet-na-2024-rik-uhvaleno.
Про затвердження формули розподілу освітньої субвенції між місцевими бюджетами: Постанова Кабінету Міністрів України від 27.12. 2017 р. № 1088. URL: https://zakon.rada.gov.ua/laws/show/1088-2017-%D0%BF#Text.
Про Державний бюджет України на 2024 рік: Закон України, прийнятий Верховно. Радою України від 09.11.2023 р. № 3460-IX. URL: https://zakon.rada.gov.ua/laws/show/3460-20#Text.
Про затвердження формули розподілу обсягу медичної субвенції з державного бюджету місцевим бюджетам: Постанова Кабінету Міністрів України від 19.08.2015 р. № 618. URL: https://zakon.rada.gov.ua/laws/
show/618-2015-%D0%BF#Text.
Демченко О.П. Інструментарій фінансової підтримки територіальних громад. *Економіка та суспільство*. 2021. Вип. 26. URL: DOI: https://doi.org/10.32782/2524-0072/2021-26-4
Коваленко В.В., Кулікова Є.О. Ринок банківських послуг Одещини та його вплив га розвиток територіальних громад. Науковий вісник Одеського національного економічного університету. 2022. № 9-10 (298-299). С. 70-80. DOI: 10.32680/2409-9260-2022-9-10-298-299-70-80.
Національний банк України. Наглядова статистика. URL: https://bank.gov.ua/ua/statistic/supervision-statist.
Національний банк України. Грошово-кредитна політика. URL: https://bank.gov.ua/ua/statistic/sector-financial.
Національна програма кластерного розвитку до 2027. Концепція. Орієнтири розвитку. Рекомендації. URL: http://surl.li/qsaii.
Evropian Claster Collaboration Platform. Evolution of cluster policy in Hungary - 2000-2020. URL: https://clustercollaboration.eu/news/evolution-cluster-policy-hungary-2000-2020.

Ministry of Development and Technology. National Key Clusters. URL: https://www.gov.pl/web/rozwoj-technologia/krajowe-klastry-kluczowe.
Evropian Claster Collaboration Platform. Report: Cluster programmes in Europe and beyond. URL: http://surl.li/qscip.
Щербак В. Г., Готра В.В. Напрями стимулювання інноваційної активності АПК в умовах формування кластера з урахуванням ефекту дифузії. *Вісник Київського національного університету технологій та дизайну. Серія: Економічні науки.* 2016. № 6. С. 136–148.
Ганущак-Єфіменко Л. М. Концептуальний підхід до управління розвитком високотехнологічних галузевих кластерів в національному господарстві. *Актуальні проблеми економіки*. 2015. № 5. С. 112–116.
Посібник з кластерного розвитку. У рамках проєкту ЄС «Послуги підтримки МСП в пріоритетних регіонах». EuropeAid /121495/C/SV/UA. GFA Consulting Group / Державний комітет України з регуляторної політики та підприємництва (ДКРП). Київ, 2006. 38 с.
Кучер Л.Ю., Кучер А.В., Тріпілець О.В. Зелений банкінг у системі екологічного менеджменту й ефективного фінансування екопроєктів. *Вісник ХНАУ ім. В.В. Докучаєва. Серія „Економічні науки”*. 2020. № 2. С. 309-324. DOI: 10.31359/2312-3427-2020-2-309.
АТ «Укргазбанк». Офіційний сайт банку. URL: https://www.ukrgasbank. com/eco/acredyt_comp.

DOI 10.5281/zenodo.10821908
UDC 658.155:005.915

CHAPTER 10.
IMPROVEMENT OF ENTERPRISE COST MANAGEMENT

Alevtyna PAKULINA
Ph.D. economy sciences, associate professor
Department of Economics and marketing
O.M. Beketov National University of Urban Economy in Kharkiv,
(Marshal Bazhanov Street 17, Kharkiv, Ukraine, 61002)
alevtina.pakulina@gmail.com
http://orcid.org/0000-0002-2578-9701

Abstract. The work highlights the general theoretical foundations for clarifying the essence of the concept of "costs", taking into account the current trends in the development of this category. The main classifications of expenses according to various characteristics are considered in detail. The regularities and functions of cost management, the importance of enterprise cost management for stimulating resource savings and justifying management decisions are revealed. The need to transform the cost management system at the enterprise under modern business conditions, in particular crisis phenomena in the economy, is substantiated; a systematic approach to the theoretical foundations of cost management as a factor in increasing the efficiency of the enterprise. The main methods of cost management are presented, their advantages and disadvantages are analyzed. It has been established that cost management can be defined as a system of principles and methods for the development and implementation of management decisions based on the use of objective economic laws.

Key word: costs, effective cost management, enterprise, classification, cost management method, cost, optimization

Introduction

In modern conditions, the problem of reducing production costs is particularly relevant at the micro level, since most enterprises can maximize profits mainly by minimizing costs and managing them. The cost management process at the enterprise has typical goals, principles, functions and methods inherent in any management system.

Because business costs are the use of resources determined by factors of production, cost management is closely related to managerial decisions about any factor. Considering the management process as a whole, it is ultimately aimed at achieving the ultimate goals of the organization with the help of certain methods and methods.

The need for cost management arises directly from their role in the economy of the enterprise, in particular from their direct participation in creating profit for the enterprise. The final profit is the main condition for the competitiveness of the enterprise, which allows to expand the reproduction and realization of the social function of the enterprise. It is the profitability potential, which is largely determined by the company's ability to control costs, that characterizes the value and current efficiency of the company's management.

In a market economy, the competitiveness of enterprises largely depends on the quality characteristics of manufactured products, their compliance with the needs of consumers and buyers, as well as the price of these products, the ability of the enterprise to provide buyers with an equivalent product in terms of quality and at a lower price.And the ability to manipulate prices and offer different types of discounts to customers depends on the cost of products, the level of production and sales costs.

Production costs depend on many factors, both external and internal. To achieve the best results with minimal costs of production resources, it is necessary to adapt to external factors and influence internal factors. The cost of a product does not always determine its price. Prices are determined by the market, business is forced to adapt to market requirements. And for this, it is necessary to create and ensure the effective functioning of an integrated system of cost management for the production and sale of products, works and services, which corresponds to the modern conditions of the functioning of the economy of Ukraine. Therefore, the study of the main problems of the formation of such a system is extremely relevant both for economic theory and in economic practice.

A peculiarity of the researched problem is that in many works of domestic and foreign scientists and practicing economists, attention is paid to certain areas of its research. In particular, many studies are devoted to budgeting and management accounting.

However, the study of the various methods of enterprise cost management in relation to each other has generally not received enough attention, and many obvious questions have not been fully explored. Also, the characteristics of the functioning of various systems of accounting and control of production costs have not been fully studied. Therefore, special attention is paid to the application of various cost management methods for domestic business.The purpose of the study is to develop and justify proposals for the formation of an integrated cost management system, as well as the

development of scientific, methodological and practical recommendations for the effective use of modern cost management methods, focusing the attention of managers on the rational use of production resources.

To achieve the goal, the following tasks were set and solved:

– the main principles of the system approach to cost management at enterprises, scientific provisions and methods ensuring the complexity of the developed cost management system are determined;

– the composition and classification of enterprise costs according to the main features important for cost management are determined;

– the prerequisites for effective cost management were identified and analyzed, ensuring the interest of all management levels in the rational use of production resources;

- the domestic and foreign experience of using various accounting and cost control systems is summarized, the features, advantages and disadvantages of each system are determined, the conditions for their effective use in modern conditions are determined;

– the interaction of various cost management methods, their organic relationship with the key role of establishing cost standards is highlighted.

Classification of costs for management decision-making

Simultaneously with the development of production, both economic science and the practice of cost research developed.

The idea of enterprise costs is based on three important postulates:

– costs are determined by the use of resources, reflecting how many and what resources were used for the production and sale of the product during a certain time;

- the amount of used resources can be expressed in kind and monetary units, however, economic calculations use the monetary expression of costs;

- the determination of the cost price is always related to a specific goal, tasks, that is, the amount of used resources in monetary terms, calculated in accordance with the main production function and its implementation as a whole for the business or for the production department of the enterprise.

Expenses represent an outflow of economic benefits during the reporting period in the form of a decrease or use of the enterprise's assets or an increase in liabilities, which leads to a decrease in capital, except for the distribution of capital among the participants of the enterprise. The actual cost price is the cost of manufactured products, works, and services.

In the process of capital circulation, enterprises consume and use many types of materials, labor and finance for the reproduction of fixed assets and working capital, production and consumption of products.

In the process of realization of factors of production, their various combinations and their interchangeability are observed. This is due to their limitations and the need for efficient use, as well as the type and nature of the products being produced.Industrial resource consumption is carried out with the aim of creating a useful product that satisfies human needs. Product production costs make up the largest share of enterprise costs. Skillful cost management based on quality processing of this information contributes to increasing the efficiency of each business unit.

At each stage of the cycle, the business entity bears costs. Expenses should be understood as the obvious expenses of the enterprise for a certain period of time. Costs are the cost of resources (materials, labor, financial and other resources) used for specific tasks. Expenses can be shown on the balance sheet as assets that can generate future income, or as expenses of the organization. Expenses of the organization are all expenses that during a certain period of time in the process of economic activity lead to a decrease in the organization's assets and income. Only those that participate in the formation of profit during a certain period of time are considered expenses, and the rest of the expenses are capitalized into the assets of the enterprise in the form of finished products, work in progress, objects of unfinished construction, intangible assets, etc.

Product costing or product costs are carried out for the production of the planned quantity and type of products in a certain period. For trade enterprises, the cost price will be the costs of purchasing goods for further sale, and for industrial enterprises - the costs of the production of finished products.Products actually sold during a certain period include a portion of costs that are transferred to the expense category of the reporting period and shown as cost of goods sold in the income statement. The remainder of the cost of production is allocated to commodity values and accounted for in the corresponding item of the balance sheet. As a result, expenses for a certain period (financial statements) may not cover all expenses incurred, for example, in a year. It was mentioned earlier that the basis of the company's effective work in the long term is a sustainable competitive advantage, one of the most important of which is low costs. Therefore, some authors call cost management a special part of production management, which is characterized by complexity and a large number of problems to be solved.

According to the composition, economic purpose, specific weight in the total amount, role in the production and sale of the product, production costs vary widely depending on the volume of production and other characteristics. This necessitates the grouping of costs according to certain criteria, therefore their scientifically based classification is of great importance for studying cost

behavior and the possibility of cost management, choosing accounting systems, collecting accounting information and analysis. The organization of reasonable accounting of the cost of production requires a clear and justified classification of expenses.

The classification of production costs objectively shows the existing groups of costs, cost formation processes and relationships between their individual parts. Without the classification of costs, it is impossible to solve the problem of their management at the enterprise. The complexity of the structure and the variety of cost formation processes require their division according to several characteristics. Depending on the goals and approach, there are several classifications of expenses. The classification of costs for management purposes must meet the basic requirements - to be built on the basis of characteristics that allow differentiation of costs for cost management in many different aspects. This creates prerequisites for determining the level of expenses for management objects, organization of planning, accounting, control and analysis.

Depending on the volume and variety of produced products (works, services), production costs are classified mainly by type of activity (type of production). According to this criterion, the following production groups are distinguished: main production, auxiliary production, service production.The main industry is defined as production activity related to the production of products for which the organization was created. The products of the main production industry are intended for sale on the market, therefore, they are of crucial importance for the economy of the enterprise. Auxiliary production is designed to ensure the normal operation of the main production. Service sectors are mainly engaged in the provision of social services to their employees and partly to people living on the territory of the organization.

Production cost formation zones characterize different levels of product cost (works, services) in order to determine the financial results of activities, prepare reliable accounting (financial) reporting, and also serve for management purposes. The formation of production costs, which is included in the cost of manufactured products (works, services), is carried out in construction organizations according to the following components:

– cost of materials;

– salary expenses;

– social needs;

– depreciation;

– other expenses.

Costs of raw materials and materials in the process of production of products (works, services) represent material costs. According to their purpose and use in the production process, raw materials and materials are classified according to the type of material and production and production services.

According to the method of acquisition, materials and raw materials are divided into purchased and self-produced. The "Material costs" component reflects the cost of labor items (used in production), maintenance costs and production work of construction organizations.The component "Labor costs" reflects the labor costs of all categories of personnel in the organization, based on piece rates, rates and salaries, established depending on the results of work, quantity and quality, incentives and remuneration, including payments, etc. related to price increases and income adjustments in accordance with the provisions of current legislation; the regime of awarding production workers, managers, specialists and other employees based on production results, other terms of remuneration corresponding to the forms and systems of remuneration used in the organization.

The expense component "Deductions for social needs" has been allocated to reflect mandatory deductions of the single social contribution based on the costs of employee wages, which are included in the cost of production.

The "Depreciation" element includes depreciation expenses for the complete restoration of fixed assets and intangible assets of the organization, which is carried out in the manner determined by the accounting policy of the organization.

The element "Other costs" represents various types of costs as part of the price of products (works, services), reflecting costs that are not included in other elements (rent, rewards for inventions and rationalization proposals, travel expenses, taxes and fees in the cost of products, deductions for reserves of future expenses, expenses of future periods).

The classification of costs considered above is mainly aimed at the formation of various types of product costing (works, services). However, this is not enough for effective production management. Obtaining sufficient information for decision-making is achieved by grouping costs according to the following groups: variable and permanent, relevant and irrelevant, explicit and alternative, irreversible, marginal and other special.

Depending on whether to take them into account when making a particular decision, costs and revenues can be relevant and irrelevant. Relevant costs and revenues are future costs and revenues that are taken into account when making a specific decision, and their amount depends on the decision made. Those costs and revenues, the value of which does not depend on the decision being made, are not relevant (relevant) and are not taken into account when making a decision.

The concept of avoidable and non-avoidable costs is directly related to relevant and irrelevant costs.Avoidable costs are costs that can be avoided using other alternatives. Unavoidable costs cannot be prevented. When making optimal decisions, costs that can be avoided are taken into account.

As a result of a previous decision, costs may have been incurred that cannot be changed by any future decision. Such costs are called sunk costs and are not taken into account when making new

decisions. Suppose three years ago equipment was purchased for 500,000 hryvnias, and depreciation was accrued for this amount during this period. Currently, the residual value of the device is UAH 200,000. The residual value of the equipment itself is a sunk cost that will not affect future decisions to replace that equipment. For example, sunk costs include the value of illiquid assets. Although both sunk and sunk costs are ignored in decision making, these costs are not the same. Sunk costs are costs of a previous period, and the concept of relevance is tied to the future.

For management decision-making, it is important to separate costs into explicit costs and substitution costs. Explicit (actual, accounting) costs are costs incurred by the organization in the process of production and sale of products (works, services). Opportunity costs arise in conditions of limited resources when choosing an alternative from several options. They represent lost profits when choosing one action prevents another from occurring. Opportunity costs occur when resources are limited. If resources are unlimited, then opportunity costs are zero.Estimated costs are always additional costs attributed to their accounting object, even if the actual main activity is not reflected in the accounting. Not paying attention to them and underestimating their importance can lead to wrong decisions. This is especially important when calculating the cost of products, works, and services for the purpose of pricing and evaluating the effectiveness of investment projects and other future costs. Opportunity costs typically include lost profits, cost of risk, depreciation of written-off assets, capital gains, and other costs called accruals.

Any cost that occurs with any alternative but is wholly or partially absent from another alternative is called differential. It represents different levels of costs when considering two alternatives. Differences in costs and revenues can also occur when additional units of the product are produced or sold. Such costs and revenues per unit of production are called marginal (marginal).

Of particular importance in management accounting is the division of costs related to the volume of production into fixed and variable. It is the basis for most calculations aimed at optimizing the ratio of costs and results, substantiating profit maximization of the production and sales program, the most acceptable price policy, the "direct-costing" system, measuring marginal costs, and determining marginal income.

The main criterion for classifying costs according to the degree of variability is their dependence on changes in the volume of activity associated with these costs. The amount of fixed costs does not depend on the volume of activity and does not change when it increases or decreases. Variable costs in the total amount change according to the increase or decrease in the volume of production (revenue) and the level of utilization of production facilities.

Determination of factors and ways to optimize enterprise costs

Factors that determine the amount of costs of production and consumption of the company's products can be divided into two main groups: external to the company, independent or less dependent on the company's activity, and internal, dependent on economic activity.

External factors include prices and tariffs for raw materials, materials, works and services used by the enterprise in the production and sale of products, the minimum salary of personnel in accordance with the legislation of Ukraine, as well as such as taxes and contributions to extrabudgetary funds, which are included in the cost price products (works, services) of the enterprise.

External factors that determine the company's costs depend on inflationary processes in the country's economy and the ratio of supply and demand for material resources and labor on the market. The ratio of demand and supply is not the same in different regions of the country, so enterprises must constantly monitor the market situation and try to purchase raw materials, hire workers and specialists at minimum prices and wages. This means that business behavior when considering the impact on costs depending on external factors should be proactive.

Internal factors include the efficiency of using enterprise resources (labor, materials, fixed assets) and the volume of production and sale of products (works, services).

Internal factors are the main factors that determine the company's costs, which are completely dependent on the qualifications and efficiency of the company's personnel.Internal factors that help reduce business costs include:

- the composition of the product, which requires minimal consumption of raw materials;
- a resource-saving production technology that requires minimal labor, material and energy costs;
- distribution of consumption of all resources used by the enterprise;
- the ability to organize production, ensure a reasonable amount of unfinished costs, high workload of equipment and eliminate non-production costs of the company's resources;
- the ability to use technological devices, especially expensive devices, in cost-effective directions;
- rationalization of the organizational structure of the production management system, which leads to a decrease in management costs;
- an effective system of economic relations in production, which contributes to the saving of all types of resources;
- the ability to organize work, to exclude loss of working time during the day and shifts, to ensure high labor productivity and saving of labor costs;
- the ability to organize the infrastructure for production support and maintenance, to create conditions for the effective operation of economic entities with minimal costs;

- technological discipline in production, ensuring product quality and eliminating costs due to errors;

- accounting for the cost of production, provision of accurate, timely and reliable information on the costs of production and sale of products (works, services);

- a perfect cost management system at the enterprise, including planning, accounting, control, analysis and determination of responsibility for compliance with established costs.

Internal factors of business cost reduction include the growth of production volumes (works, services). The reduction of the company's costs occurs due to the saving of the company's fixed costs, the value of which does not increase with an increase in the volume of production and a decrease in the amount of the company's fixed costs per unit of production. This reduction in costs is very important for determining the cost price of the enterprise's products when increasing the volume of production and sales.

Determination of provisions and coordination of work to reduce costs of the enterprise is carried out by economists and managers of production and functional departments of the enterprise and managers of the enterprise, production department.

The task is to choose an appropriate incentive system to encourage the company's employees to reduce costs. Stimulation (motivation) is an influence on the consciousness of people, which contributes to the formation of motivation for them to achieve certain goals and tasks. There are moral and material incentives. The system of material incentives should ensure the improvement of the work efficiency of this group of employees and should be built in such a way that the bonus depends on the productivity, quality and saving of materials, that is, the indicator contributes to the reduction of final costs. Every employee can and should feel a close connection between their performance and their reward.There are rules that must be followed when building a material incentive system:

- the system should provide every employee with the opportunity to participate in increasing labor efficiency;

- the amount of the bonus should be made depending on the factors that the employee can directly influence;

- representatives of all interested groups should participate in the development of the system.

The effectiveness of the influence of the stimulation system is guaranteed by following the following principles:

- set clear goals (clear definition of the results to be achieved through incentives, the level and composition of costs, reductions that employees can influence);

- use well-thought-out, reasonable and acceptable measurement and evaluation criteria;

- a strong connection between incentives and results in terms of volume and time;

- apply moderate standards, monitor them and have mechanisms for changing them;

- compliance with the "sensitivity threshold" of the stimulation system.

Depending on the employee's position in the production process and his ability to reduce costs, different incentive systems can be used.

Many enterprises in their activities use a strategy of reducing costs, in the framework of which employees take the following steps: study the factors that affect the level of costs; check compliance with technological process standards; calculate the optimal load of production shops; find out the reasons for interruptions in work; monitor the presence of defects during shipment or receipt of goods; determine warehouse overload. After that, costs are analyzed and optimized.In other words, employees develop a program to reduce identified costs, which is then reviewed by management.

In addition, cost reduction planning includes a set of activities broken down by time:

1. Compliance with financial discipline. Measures are being developed to maintain financial discipline, including strict adherence to approved financial indicators. Decisions made by the management and indicated in the estimate can be violated only in exceptional cases.

2. Organization of accounting. In order to systematically reduce costs at the enterprise, it is necessary to implement a system of financial accounting and control. It is necessary to take into account not only the costs, but also the income of the enterprise.

3. Taking professional measures to recover debts. In addition, the enterprise must timely make budget payments and settle with employees and partners in order to avoid fines.

4. Development and implementation of a cost reduction plan. The goals of this cost reduction plan are to set specific targets for each cost item that needs to be reduced. Within these measures, first of all, a general plan is developed for the entire enterprise with the identification of weak areas that can lead to cost reduction. In addition, separate measures are being developed for each division to strengthen financial discipline in this area.

5. Carrying out control checks. To assess the effectiveness of cost reduction, constant independent observation is necessary, which will allow to assess possible shortcomings, technological losses with the necessary adjustment of cost reduction plans.

6. Damage analysis. Any results, including negative ones, must be rechecked to further reduce costs.It is necessary to analyze production losses, which forces the sale of goods (services) at a reduced price. Special attention should also be paid to shortages and recycling.

Since the domestic experience in the field of cost optimization lags far behind the Western one, we will consider some methods that can be applied for this purpose: the method of using consumables; application of the Pareto law; cost comparison, charting, benchmarking, direct costing,

standard costing, ABC method (Activity Based Costing); Just in Time system, target costing; kaizen costing; LCC analysis, functional cost analysis, SCM method.

The method of using consumable media. This is the simplest of the cost analysis methods, and it focuses on the study of the factors and causes that affect the amount of costs. The analysis of cost carriers according to the production and economic processes of the enterprise helps to find reasonable solutions and optimize costs.

Application of the Pareto law. The most important categories of expenses are highlighted, since only they provide significant savings. To achieve 80% of the effect, it is only necessary to determine and optimize those costs that make up the largest share, namely 20%. This means that in order to obtain significant cost savings, efforts must be directed to significant optimization of these key cost items.

Cost comparison, charting, benchmarking. Benchmarking (Benchmarking) is a system of evaluating the company's activity by comparing it with relevant analogues.This method allows you to identify the strengths and weaknesses of the enterprise's cost process by comparing it with the best practices of other companies in the relevant industry. Benchmarking results can serve as a basis for implementing improvements and cost optimization. Trend analysis on cost charts. This method involves visualizing costs using charts, graphs, or other visual aids. Trend analysis on cost charts helps identify changes in costs in previous periods, identify significant costs, identify deviations and their causes. This allows you to develop further measures to eliminate the causes of deviations and optimize the cost process.

Direct-costing is a method of accounting in the controlling system, which is based on determining the true cost of products and services, regardless of the estimated fixed and overhead costs. This system provides for accounting of the cost price only in the part of variable costs. Fixed costs are aggregated on separate accounts and reflected directly in the financial results with a certain periodicity.

The main advantage of the direct costing system is the ability to manage the business. The problem is that quite often companies measure their performance in terms of profitability at the end of the period. It may be a year, a quarter or a month, but for a growth company, even with a decline in operational efficiency, profits can continue to grow, offset by increased sales. As a result, if such companies begin to lose profits, it indicates problems so large and advanced that it may be too late to address them. Secondly, the market is always dynamic and it is important to understand exactly how this or that structural unit works at the moment. Direct-costing allows you to solve these really important problems and manage the company not on the basis of profit or revenue, but on marginal profit.

The direct costing system has the following features:

- distinguishing between variable and fixed costs: depending on their variability relative to the volume of production;

- fixed overheads are not included in the cost of products: in the direct costing system, fixed overheads are not taken into account when calculating the cost of products.They are directly credited to the profit and loss account for the corresponding period when they were incurred.

Standard costing (standart costing) is a cost accounting and costing system that uses normative (standard) cost. "Standard" - the amount of costs necessary for the production of one unit of production; "costing" is the monetary expression of these costs.

The main features of the standard costing system include the following:

- the presence of a system of standards, when rules, norms and standards are established, which serve as the basis for determining the cost of resources for the production of products. These standards are regulated and documented for each type of expenditure;

- determination of a reasonable rate of resource costs, when a reasonable rate of resource costs per unit of production is established for each type of costs, such as material, labor, etc. This makes it possible to establish the standard production cost of a product unit.

- calculation of deviations, when resource costs according to norms and deviations from norms of resource costs are calculated separately. The analysis of actual costs is compared with regulatory standards, which allows for deviations to be detected and appropriate corrections to be made.

The ABC method (Activity-Based Costing) is an effective approach to accounting, analysis and optimization of process costs. It helps enterprises calculate the costs and productivity of operations with high reliability, as well as determine the efficiency of the used resources and calculate the cost of the product. Compared to traditional costing approaches, the results determined using the ABC method can be significantly different.The explanations are that the ABC method allows for a much more accurate assessment of costs, their allocation to specific activities and accounting objects. Such a detailed approach allows you to get a more objective picture of costs and use of resources in various processes of the enterprise.

The Just in Time (JIT) system, known as "just in time", is revolutionizing production using a unique principle: to produce products only when they are needed, in limited quantities. This method is based on the logistical concept of "nothing is produced until it is needed", which allows for extraordinary efficiency in production management. In the Just in Time (JIT) system, mass production of products in large batches is abandoned. Instead, production is carried out in small batches according to current demand. This approach helps reduce inventory because products are made only when they are needed. The Just in Time (JIT) system allows enterprises to eliminate unnecessary

costs through efficient production management. This approach aims to avoid overproduction, downtime of equipment and personnel, unnecessary warehousing, and costs associated with product defects. In the framework of JIT, the demand for the product accompanies its production without excess stocks, and materials are delivered exactly when they are needed in the production process. This allows you to focus on the quality of the product, its availability and overall value, instead of the simple purchase price.

Target Costing (Target Costing) – determining the cost of a new product, based on the planned market price and expected profit from sales. It is used in creative industries, at enterprises where new categories of products are always being created.

Target-costing is an interesting strategy that goes beyond traditional cost accounting.At the heart of this concept is a review of the relationship between price, profit and cost. Instead of the traditional approach, the target costing algorithm assumes that the new product will be sold at a price that will cover its costs and provide the necessary level of profit to continue the business. In the target-costing system applied to traditional products, the order of actions and the priority of the components in the expression have been changed. Now the main emphasis is on achieving the target price by determining the target costs that can be covered by the price of the product and bring the required level of profit. Thus, the formula changes to the following: target costs = target price - target profit.

M. Sakurai in 1989 defined target cost as a cost management tool used to reduce costs associated with a product throughout its life cycle. This concept emphasizes the complexity and complex nature of target costs, combining the efforts of the company's production, design, research, marketing and economic divisions.

The main characteristics of the target-costing system:

- determination of the target cost price based on the sales price and the desired level of profit, involving all units of the enterprise. It is a strategic cost management tool.

- horizontal interaction between functional parts of the business, which contributes to joint efforts to achieve the target cost price.

- constant use of the target-costing system at various stages of the product life cycle.- organization of ongoing cost control to ensure compliance with the target cost price.

- relevant marketing forecasts and accurate positioning of the business on the market to establish realistic goals and parameters of the target-costing system.

Kaizen costing (Kaizen Costing) is a constant and continuous reduction of costs as a result of the implementation of a specific enterprise program. This method is based on reducing the time spent on activities that do not increase the "cost" of the product being produced (accumulation, movement, storage operations).

Kaizen costing and target costing are two components of the Japanese management accounting model that work in parallel to achieve target cost. Target costing is determined at the design stage of a new product, while kaizen costing is used at the product manufacturing stage. If the estimated cost shows a difference of up to 10% compared to the target cost at the design stage, then production is started with this 10% difference, assuming that it will be eliminated during the production process using the kaizen costing method. This method is the process of reducing the difference between estimated and target costs, and it involves all employees of the enterprise, from engineers to managers. This process is actively supported by the personnel management system, which stimulates its proper execution.

A kaizen task is set during planning for the next fiscal year, when production plans are developed. It can be delivered both for a single product and for the entire business, taking into account variable costs. Fixed costs are calculated for each department and combined into special budgets. With the help of a kaizen task and a budget of fixed costs, experts draw up the company's annual budget.The main features of the kaizen costing system:

– focuses on continuous and integrated cost reduction, not on achieving a certain cost level.

- ensures achievement of target costs in the production process.

– is used mainly in the operational management of costs and control of their level.

- implies constant use and application.

- implementation of small, but constant improvements in production processes, which can lead to significant results in general.

- involves all employees in constantly improving the quality of work and creating the necessary motivation system.

LCC analysis (life cycle cost analysis) is a unique method that is based on the assessment of the cost of a product throughout its life cycle, which includes the stages of development, promotion, sale, maturity and withdrawal from the market. This method provides a comprehensive analysis of technology for various purposes, including a complete analysis of planning, budgeting, contracting and investment real estate, as well as a detailed analysis that includes a thorough assessment of financial parameters, such as real estate acquisitions and conducting technical studies using new technologies. The advantage of this approach is its uniqueness in the ability to compare actual information about costs with previously planned, create a statistical database, evaluate the impact of costs on innovative business processes and, above all, take into account the benefits of the product for consumers.

Functional Cost Analysis (FCA) is based on a functional approach, which involves studying the functions of the research object and applying various algorithms and methods to achieve these

functions with the lowest costs. FCA is based on the assumption that in order to produce a certain product or provide a service, it is necessary to perform sequential actions, each of which requires the use of a certain amount of resources. Functional Cost Analysis (FCA) really involves the accumulation of the cost of each action with certain changes, which are finally taken into account in the cost of the organization's products or services. FCA is an integrated approach to studying the features of the analysis of objects, such as products, processes or structures, with the aim of minimizing costs and maximizing efficiency. To achieve this, FCA's goal is to find the optimal balance between effect and cost. Traditionally, FCA aims to achieve cost reductions of between 10 and 20%.

Functional cost analysis (FCA) is aimed at finding optimal opportunities to perform various functions with minimal costs, while ensuring high quality, safety and attractiveness of goods and services on the market. The success of FCA depends on several factors, including the support of the company's management and understanding of its capabilities. In modern market conditions, FCA is a valuable tool for solving complex economic, technical and organizational tasks faced by business entities.

SCM method (value chain).The value chain for any organization is a sequential set of value-creating activities, from raw materials to component suppliers to finished products delivered to the end consumer. Here, the focus is on processes that occur outside the company, and each organization is considered in the context of the overall value chain of activities, as part of it, from raw materials to end users.

As for choosing a specific method, the ABC method uses accurate information for pricing and forecasting, but this method is quite difficult to use on a day-to-day basis, unlike the cost carrier method, which is the simplest method. Pareto's law applies only to the most important categories, but the degree of control over an item can be a hindrance to cost management. Cost comparison methods, charts, and benchmarking have drawbacks: many businesses do not understand their cost structure; companies that do not have clear cost reduction goals; lack of economic culture as a component of corporate culture. Advantages of target costing: concentration of employees' attention on external factors to a greater extent than on internal ones. Problems: conflict of interests between departments - cost reduction is not always equally beneficial for all departments; conflicts between managers and subordinates caused by the motivation of employees. Kaizen costing, unlike target costing (target costs), is used at the production stage.And in the case of developing a strategy to increase the competitiveness of the product and the company as a whole due to obtaining a competitive advantage, the value chain approach turns out to be the best.

At the same time, the effectiveness of the cost optimization method used can be evaluated using a multi-level assessment of economic and production efficiency or a method of calculating production risk.

Content of cost management at the enterprise: essence, functions, principles, systems

The increase in the scale of enterprise activity, the integration and specialization of enterprises, the complication and increase in the number of connections between enterprises, combined with the difficult situation of the domestic economy, have exacerbated the problems of efficiency and quality of management. Management is a complex socio-economic process, in a broad sense, influencing an object or system to maintain stability or transition from a certain state to another that meets certain goals.

The main goal of management is to achieve the greatest results of economic activity with the lowest aggregate costs of living and material labor.

Cost management is a means for enterprises to achieve high economic efficiency. This is not limited to cost reduction, but also extends to all controls. Most enterprises have provisions to reduce costs to a reasonable level, which contributes to the growth of economic efficiency and competitiveness. Cost management can be considered a functional area of management and an independent area in the enterprise management system. These two approaches do not contradict each other and can be understood as the definition of cost management, which directly translates theoretical and practical management developments into the management of a specific company. From another perspective, the concept of "cost management" is narrowed down to the scope of defining the functional tasks of the relevant service.Cost management tasks in business include the need to:

- determine its role as a factor of increasing economic efficiency;
- to determine costs according to the main functions of management;
- calculate costs for each department in the business;
- calculate the necessary specific costs per unit of production (works, services);
- to prepare an information basis for cost estimation when forming and adopting business decisions;
- determine technical methods, means of measuring and monitoring costs;
- search for backup sources to optimize costs at each stage of the business process and in each link of the company;
- choosing a cost management system that meets the conditions of the enterprise.

The issue of cost management must be solved comprehensively. Using only such an approach can contribute to increasing the economic efficiency of the entire enterprise.

The success of the enterprise and its ability to compete in market conditions largely depends on how the problems of cost management that arise in the production and consumption of products are solved. Before considering the main functions of cost management, it is necessary to define what this process is and its place in general business management.

Cost management is a component of the entire management system of the enterprise. To understand their nature, let's focus on cost management functions.

Cost management functions are performed using the following elements of the management cycle:

- analysis and control;
- production cost accounting;
- forecasting and planning;
- organization;
- interaction and synchronization;
- support and encouragement of working capacity.

Cost forecasting and planning are divided into long-term (at the stage of long-term planning) and current (at the stage of short-term planning).

From the point of view of the economy, planning is one of the branches of management, which is related to the planning of the activities of the entire organization, its divisions, functional subsystems, departments, services, and employees. This is an organic part of the management process, which sets the direction and parameters of the organization's future development. In management accounting, planning is the process of determining actions to be taken in the future.

Planning in a market economy plays an increasingly important role and is characteristic of both the public and private sectors. Abroad, it is better established in private business, as evidenced by the saying of K.F. Flexner: "If private corporations were as poorly planned as the public sector, and if their employees were as inexperienced and lethargic as other government officials at various levels, our economy (we're talking about the US economy) would be much less efficient."

The concentration of production on a large scale requires on-the-spot cost planning, which is a necessary and very effective tool for organizing and managing the company's activities.The minimum results of planning are to avoid serious mistakes in economic activity, that is, to be able to foresee and eliminate unpleasant future situations in advance. Implementation of planning and its organization is the business of the enterprises themselves, but state and former state enterprises that perform traditional functions are especially in need of new planning systems.

Forecasting is the definition of a system of probabilistic goals for the functioning and development of socio-economic systems, probabilistic ways and methods of their achievement.

Forecasting is fundamentally different from planning in that it assumes the probabilistic nature of goals and ways to achieve them. Unlike other functions of management, it does not have the character of a positive influence of the subject of management on the object.

Planning and forecasting are the most important components of the business management system, which allows:

- evaluate the future prospects of the enterprise's development;
- avoid the risk of bankruptcy;
- implement the enterprise's scientific and technical policy more purposefully and effectively;
- promptly improve the quality of the products produced;
- to increase production efficiency and improve the financial situation of the enterprise.

The organization establishes how cost management is carried out at the enterprise, that is, who does it, in what terms, using what information and documents, and in what way.

Interaction and synchronization of costs involves comparing actual costs with expected (normative) costs, identifying deviations and making decisions about timely measures to eliminate them. Standard costs are values carefully calculated in advance and usually expressed per unit of finished products. Currently, many researchers believe that the first stage of the cost management process is the need to form a theoretical basis and methodology for cost regulation.

Support and encouragement of work capacity involves finding ways to influence production subjects to encourage them to fulfill the costs set by the plan and to find opportunities to reduce them. The direction of employee stimulation is the collective's material interest in increasing labor productivity, achieving the set goal to such an extent that the rate of labor productivity growth significantly exceeds the rate of wage growth.

One of the most important methods of tracking the company's activity indicators is accounting, the purpose of which is to summarize the results of activity for a certain period of time. Accounting is an information base that allows you to evaluate the effectiveness of the decision made, is the basis for planning, forecasting and decision-making.

Management requirements require the study of methods of accounting for the cost of production and the construction of a system for tracking the cost of production of basic divisions based on an extended analysis of cost groups used in the production process.

Issues of development and practical use of new methods of effective cost management are widely discussed in domestic and foreign literature.It is possible to agree with the generally accepted definition of the essence of cost accounting as "a set of conscious actions aimed at reflecting the processes of providing, producing and selling the product of labor that take place at the enterprise during a certain period of time through the process of quantitative measurement (in kind and value),

registration, grouping and analysis in parts that make up the cost of finished products". Such a display provides comprehensive information necessary for managing the enterprise and evaluating its activities by calculating financial results.

However, this approach in the context of the beginning of the development of the concept of controlling and the development of the theory of production accounting is limited in the field of use. In addition to the technical aspect, the determination of the essence of production cost accounting also includes many different approaches to the organization of management accounting of production activities. Accounting as an information flow, unlike the management process, will not only reflect reality, but also prepare information for modeling the future economy of the enterprise.

The traditional cost accounting system of domestic organizations is aimed at only one goal - calculating the cost of manufactured products and determining financial results. It does not provide data in a form suitable for making management decisions in cost and performance areas.

Cost analysis is a component of the control function, which helps to evaluate the efficiency of the use of all business resources, identify measures to reduce production costs, collect information for planning and make informed management decisions in the field of costs.The control (monitoring) function in the cost management system provides feedback when comparing planned and actual costs.

When organizing cost management, it is necessary to adhere to a number of principles that create the basis of the economic competitiveness of the enterprise and the acquisition of leading positions in the market. The principles of cost management are the most basic, general rules and recommendations that must be taken into account and followed in practice at all levels of management. The main requirement for these principles is that their adherence will increase the effectiveness of practices. The main principles of cost management were developed in practice and summarized as follows:

- a systematic approach to cost management. This principle includes the study of the management object and the management system together and inseparably. Systematicity means the need to use systemic analysis and synthesis in all management decisions. The system approach is demonstrated in the fact that the effectiveness of cost management is evaluated by the effectiveness of the weakest link in the system. Insufficient attention to one control function can spoil the entire operation. It is the weak link that determines the reliability of the entire economic system;

- unification of methods implemented at different levels of cost management. Methodological unity provides uniform requirements for information provision, planning, accounting and cost analysis. There should be uniformity and dependence of the efficiency criteria used. For this, first of all, the local criteria must depend on the criteria used at a higher level and logically follow from them.

Second, the system should use uniform criteria for evaluating similar activities.Only in this case is it possible to compare the expected and actual results when achieving similar goals and generalize them;

- cost management at all stages of the product life cycle. The life cycle is the process of creation, development, production, operation, circulation and disposal of a product. The structure of the product's life cycle, its duration, volume and quality indicators determine the company's costs. A product that is the goal of the economic process, and at the same time its result is the consumption of all elements of the life cycle. Removing a phase from the life cycle does not mean reducing costs;

- an organic combination of cost reduction with high quality products (works, services). In the conditions of a market economy, the most important condition for business survival and development is the production and consumption of competitive products, which is achieved by combining quality and price. The contradiction is that high product quality, along with increased competitiveness, increased sales and increased business market share, also leads to higher costs and higher prices. The optimal balance between quality and cost at all stages of the product life cycle is achieved thanks to competent management based on research and economic calculations;

- avoiding unnecessary costs;

- widespread use of effective cost-saving methods;

- improvement of information support on the level of costs;

- increasing the interest of all business departments in reducing costs.Considering the variety of types of costs at different levels of production and management in construction, their close association in operating enterprises, it is possible to highlight and substantiate the main principles of cost management in construction.

The principle of purposefulness provides for the establishment of strategic and tactical goals in the field of product cost management of both the construction enterprise and its structural units (responsibility centers).

The principles of information security require the use of objective and timely information at all levels of management.

The principle of resource substitution provides for the possibility of using different combinations of resources for the production of a certain type of product.

The principle of the interest of production divisions of enterprises in reducing costs is to ensure and create a system of motivating employees based on the final results of their activities.

The principle of organizational innovativeness and production and technical equipment contributes to the effective development of scientific, technical and innovative potential to create economic conditions for the production and consumption of competitive high-tech products.

The principle of organic combination of high quality products (works, services) with an acceptable cost price consists in the need to link quality costs with the final results of production activities (the amount of income, profit, etc.).

The principle of unity of methods at different levels of cost management provides for uniform requirements for information provision, planning, accounting and analysis of costs at the enterprise.

The principle of accounting for the stages of the product's life cycle requires taking into account costs at all stages of the life cycle. Implementation of cost management principles creates a basis for increasing business competitiveness.

In modern economic conditions, one of the effective cost management tools of the enterprise is the "standard-cost" system, based on the principles of accounting and controlling costs within the established levels and standards and on the basis of deviations from them.Since its creation, the standard cost accounting system has successfully developed and is now widely implemented by many leading companies in countries with developed market economies.

The term "standard cost" includes two words: "standard", which means the sum of production costs (materials, labor) to produce a unit of a product or a pre-calculated cost to produce a unit of a product or supply a service, and the word "cost" refers to the cost of a unit of a product. Thus, the standard cost in the full sense of the word means a normative cost.

The meaning of the "standard-cost" system is that what will be included in the accounting, and not what happened, it is necessary to take into account not what is, but what should be, and the deviations that arise will be reflected separately. The main task that this system sets before itself is to take into account losses and deviations in the company's profits.

The basis of the "standard-cost" system is the preliminary (before the start of production) distribution of costs by cost categories. Precalculated rates are considered fixed rates to bring actual costs in line with standards through skillful business management. In the event of deviations, regulatory standards will not change, they remain relatively stable throughout the specified period, except for significant changes caused by new economic conditions, significant increases or decreases in raw material and labor costs, or changes in production conditions.The difference between actual and estimated costs arising in each reporting period will be accumulated during the year on separate difference accounts and will be fully accounted for not in the cost of production, but directly in the financial results of the enterprise.

Costs calculated according to standard regulations serve as the basis for production operations and cost management. On the basis of established standards, it is possible to determine in advance the expected costs of production and consumption of products, calculate the unit cost of production to determine the price, and at the same time draw up a report for the next year. Deviations from

established cost standards are regularly analyzed to determine their causes. This allows management to promptly correct production problems and take measures to prevent them in the future.

The most important thing in calculating according to standards is control over the most accurate definition of deviations from established standards, which contributes to the improvement of these standards. In the absence of such control, the use of standard costing will be conditional and will not bring the proper effect. Using a standard costing system gives the organization several advantages:

- standards are developed as a basis for planning the organization's activities in the short and medium term;

- through cost distribution, cost control is established and possible losses due to inefficient use of resources are minimized;

- the normative cost per unit of the calculation object is a guideline for product pricing;

- analysis of deviations of actual costs from normative ones helps to identify bottlenecks in the organization's activities and make reasonable management decisions;

- reducing the number of accounts in comparison with the historical cost reduces labor intensity and simplifies accounting, since in this system accounting is conducted according to the principle of exception, that is, only deviations from standards are taken into account.

Managers of foreign companies and companies use the standard cost accounting system as a powerful tool for controlling production costs and calculating cost, as well as for management, planning and making the necessary decisions.

Controlling is an enterprise management system aimed at achieving the ultimate goals of the enterprise. Controlling is carried out according to the principles of the "standard costing" and "direct costing" systems.It provides management of production processes to achieve business goals, maximum use of available resources and production efficiency, elimination of possible errors and deviations. With the help of controlling, it is necessary to solve the following management tasks:

- participate in the development, coordination and analysis of plans drawn up by structural units;

- create planning methods and link divisional plans with regular corporate plans;

- regularly monitor the execution of planned tasks;

- determination of methods and measures to promote the implementation of the plan's tasks;

- develop the necessary indicators for parameter analysis;

- identify deviations from planned goals, norms and standards by comparing established parameters;

- establish the permissible limits of deviations from the plan;

- determine the causes of deviations and the manager responsible for them;

- develop proposals for eliminating negative trends;

- consultation on the selection of corrective measures based on the developed proposals.

Collection of the most important information for management decision-making is a constituent part of tasks performed by control activities. To solve these problems, it is necessary to create independent analysis and control centers at the enterprise, which should be the dispatching service of controlling.

There are two levels of controlling - strategic and operational. Strategic controlling is the most important component of controlling, management of the external environment, factors of strategic success, alternative strategies and strategic goals.Such controlling is aimed at the implementation of long-term strategies and programs. Its purpose is to form a management and planning system that ensures the movement of the enterprise towards the set strategic development goals. Strategic controlling is designed to ensure effective business survival in the long term. The following tasks of strategic controlling can be distinguished:

- set qualitative and quantitative business goals;

- responsibility for strategic planning;

- to develop a system of alternative strategies;

- to determine the critical points of the external and internal environment for building a system of alternative strategies;

- identification of bottlenecks, search for weak points and ways to eliminate them;

- formation of a system of indicators for the control and information system;

- manage deviations of actual indicators from planned indicators (standards);

- dynamic system management;

- management of the economic potential of business.

Operational controlling is related to the creation and maintenance of the level of efficiency in achieving the current system of local goals of the enterprise and effective management of the enterprise. The peculiarity of such controlling is, first of all, the focus on planning current operations; secondly, it is the basis of strategic controlling and strategic planning; third, it solves more local problems than strategic control.

Strategic controlling differs from operational controlling in the following features:

- unlimited planning period;

- strategic control work has indicative value;

- calculation and systematization of the influence of all important external factors on the enterprise, its weaknesses and strengths and systematic control of their development;

- risk assessment taking into account the available resources (capital, personnel, machine arsenal);

- implementation of planned strategies and integration of these plans into operational control.

Cost management is one of the key elements of controlling.

The goal of creating new cost accounting systems is to obtain accurate, timely and reliable information for controlling operations and analyzing the profitability of certain types of products and processes. These goals are also served by the total cost management system (Total Cost Management - TCM), designed to manage all resources and types of business in the process of resource consumption.

In the TCM system, the main role is given to the development and implementation of a special method of cost accounting by activity types - activity-based costing (English Activity - Based - Cost - ABC).The essence of this method is as follows: saving resources is an effective way to reduce costs. Cost management should ensure a real reduction by reducing non-value-added activities and improving those activities that create value, that is, increasing the value of the product. The ABC system method can be defined as follows:

- unlike the traditional accounting method, which is based on the placement of production products that consume resources, the ABC system is based on the principle: products consume activities, production activities consume resources;

- to determine costs, cost formation factors (so-called cost drivers) are determined, which connect specific types of activities and corresponding costs and serve as a measure of activity, since costs change proportionally to the scale of activity;

- on the basis of cost drivers, resources are allocated among centers of production activity and then allocated to specific products.

The ABC system provides calculation of the cost of each type of product at each stage of the production process. This lays the foundation for cost management of production centers and final cost analysis of specific products. As experience shows, a reliable determination of the cost of specific products significantly increases the objectivity of the assessment of product profitability. The reality is that traditional methods of allocating overhead can distort profits.They do not reflect the increase in costs for products produced in small series, since they account for a smaller share of total production costs. On the contrary, products produced in large quantities carry a larger share of overhead costs and are less profitable.

Conclusion

During the implementation of the research, in accordance with the tasks and goals, the results were obtained.

The paper covered key issues such as the essence and types of costs, the main principles and tasks of cost management, as well as methods of cost optimization to ensure the efficiency of the enterprise.

A careful analysis of the obtained results allows us to draw the following conclusions. First of all, it should be noted that costs are an integral part of enterprise management, and it is necessary to manage them effectively, which is an important condition for the successful functioning of the enterprise. The second aspect is that cost optimization is a necessary element of effective enterprise management, and achieving optimal cost control is key to the successful operation of the enterprise. In addition, it can be determined that the classification of costs is carried out according to various criteria, including functionality, chronological aspect and their relation to production. This provides an opportunity to consider their features and set priorities in managing these costs.

Optimizing costs at the enterprise consists in creating a harmonious balance between reducing costs and providing adequate resources for the efficient functioning of the company. For this, monitoring of expenses, systematic planning of their level, optimization of business processes are used.

Cost monitoring strategies allow you to avoid unnecessary costs and improve resource management. Systematic planning helps to carefully determine financial resources, their distribution and use in accordance with the strategic goals of the enterprise.Optimizing business processes involves constant improvement of production and management procedures to achieve maximum efficiency. The search for alternative resources may include the use of the latest technologies, the search for cheaper suppliers, or the consideration of alternative production options. This comprehensive approach helps businesses remain competitive, maximize resource utilization, and achieve sustainable financial success.

The application of the cost function becomes a key element of the company's cost optimization. This strategy provides an opportunity to analyze, forecast and make informed decisions about the efficient use of resources.

Based on the analytical summarization of information on the company's expenses, several potential areas of cost optimization can be identified:

- optimization of procurement activities (verification of alternative suppliers and establishment of long-term contracts to obtain better conditions for the price and quality of materials and services);

- energy efficiency (implementation of measures to reduce energy consumption, such as installation of energy-efficient equipment, optimization of heating and lighting systems, control over energy costs);

- inventory management (optimizing the level of inventory of materials and components by implementing an effective inventory management system, accurate demand forecasting and optimal supply planning);

- process optimization (detection and resolution of deficiencies in production processes, elimination of redundant operations, reduction of production cycle time, automation of some processes);

- management of labor costs (analysis of work processes and rationalization of working hours, effective planning of the work schedule, assessment of labor productivity and optimization of the number of personnel);

- use of information management technologies (implementation of modern cost and financial management systems, automation of cost accounting and control over them, use of software solutions for management of planning, budgeting and analysis).

It is necessary to create a clear tactic and strategy regarding the behavior of expenses, to implement effective accounting and monitoring systems, to attract highly qualified specialists for successful management of the company's expenses.

References:

Artamonova N.S., Akulyushyna M.O. (2018) Upravlinnya vytratamy: navch. posib. / N. S. Artamonova, M. O. Akulyushyna, – K.: Tsentr navchal′noyi literatury, 2018. – 120 s.

Akhnovs′ka I., Bolhov V. (2020) Upravlinnya vytratamy: navchal′nyy posibnyk / I. O. Akhnovs′ka, V. YE. Bolhov. Vinnytsya: DonNU imeni Vasylya Stusa, 2020. 156 s. URL: http://surl.li/reins

Borysyuk I.O., Semenyaka Y.V. (2017) Formuvannya systemy upravlinnya vytratamy pidpryyemstva. «Modern Economics». Elektronne naukove fakhove vydannya z ekonomichnykh nauk. 2017. №6 (2017). S. 15-23. URL: http://surl.li/reiqi

Kostets′ka N. (2021) Upravlinnya vytratamy na pidpryyemstvakh v umovakh ryzyku / N. Kostets′ka // Ekonomika ta suspil′stvo. – 2021. – №34. URL: http://surl.li/reioo

Krot Y.M., Pasternak Y.P. (2018) Formuvannya efektyvnoyi systemy upravlinnya vytratamy pidpryyemstv. Visnyk KHDU. Seriya «Ekonomichni nauky». 2018. Tom 2. № 28 (2018). S. 148-151. URL: http://surl.li/reipa

Lytovchenko O.Y. (2019) Upravlinnya vytratamy na pidpryyemstvi: teoretychnyy aspekt. Infrastruktura rynku. 2019. Vypusk 31. S. 301-309. URL: http://surl.li/ocudy

Oliynyk T., Zaytseva K. (2019). Systema upravlinnya vytratamy pidpryyemstva /T. Oliynyk, K. Zaytseva // Molodyy vchenyy. – 2019. – № 11 (75). – S. 563 – 566 URL: http://surl.li/reipo

DOI 10.5281/zenodo.10821925
UDC 351.862.4(477):005.932

CHAPTER 11.
THEORETICAL PRINCIPLES OF PUBLIC-PRIVATE PARTNERSHIP MANAGEMENT IN LOGISTICS SECURITY FORCES OF UKRAINE

Serhii PISAREVSKYI
PhD in public administration,
senior lecturer of the Department of Logistics Management of the Operational Faculty,
National Academy of the National Guard of Ukraine
(Kharkiv, 3 Zahysnykiv Ukrainy Maidan),
psv021180@ukr.net
https: //orcid.org /0000-0002-2537-0767

Abstract. The theoretical principles of public-private partnership management in the logistical support of the security forces of the security and defense sector of Ukraine have been studied. The stages of formation and functions of public-private partnership in Ukraine are studied. The task structure of the logistical support system of the security forces of Ukraine is characterized. The role and place of state management of the public-private partnership in the logistical support of the security forces of the security and defense sector of Ukraine is defined. It has been established that clear norms and rules for the organization of public-private partnership in Ukraine have been defined. However, a certain list of spheres of implementation of public-private partnership is too narrow. Therefore, the decision-making process regarding the application of public-private partnership mechanisms in the field of state security is too complicated and not devoid of a corruption component.

Key words: public administration, public administration mechanism, public-private partnership, logistical support, security forces, security and defense sector of Ukraine, service and combat activity, security provision, crisis situations.

ТЕОРЕТИЧНІ ЗАСАДИ УПРАВЛІННЯ ДЕРЖАВНО-ПРИВАТНИМ ПАРТНЕРСТВОМ У ЛОГІСТИЧНОМУ ЗАБЕЗПЕЧЕННІ СИЛ БЕЗПЕКИ УКРАЇНИ

Анотація. Вивчено теоретичні засади управління державно-приватним партнерством у логістичному забезпеченні сил безпеки сектору безпеки і оборони України. Досліджено етапи становлення та функції державно-приватного партнерства в Україні. Охарактеризовано

структуру завдання системи логістичного забезпечення сил безпеки України. Визначено роль та місце державного управління державно-приватним партнерством у логістичному забезпеченні сил безпеки сектору безпеки і оборони України. Встановлено, що визначено чіткі норми та правила організації державно-приватного партнерства в Україні. Проте певний перелік сфер реалізації державно-приватного партнерства надто вузький. Тому процес ухвалення рішення щодо застосування механізмів державно-приватного партнерства у сфері безпеки держави надто складний і не позбавлений корупційної складової.

Ключові слова: державне управління, механізм державного управління, державно-приватне партнерство, логістичне забезпечення, сили безпеки, сектор безпеки і оборони України, службово-бойова діяльність, забезпечення безпеки, кризові ситуації.

Вступ. Сьогоднішній розвиток українського суспільства все частіше демонструє виникнення кризових ситуацій, що загрожують національній безпеці. Злиття світових цивілізацій та інші глобалізаційні процеси постійно супроводжуються збройними сутичками – цьому є безліч доказів в останніх збройних конфліктах та терористичних актах. На жаль, Україна не є виключенням в цьому гострому проблемному питанні. В умовах збройного протистояння на території України постійно виникають кризові ситуації.

Збройна агресія проти України у 2014 році, включаючи незаконну окупацію Криму і Донбасу, а також широкомасштабне вторгнення у 2022 році російських військ стали поштовхом для масштабних і структурних реформ у сфері безпеки України. Головним напрямом цієї стратегії є поступове реформування сил безпеки сектору безпеки і оборони України до стандартів ЄС та НАТО. Тому сьогодні сили безпеки України рухаються шляхом реформування та розбудови за зразком безпекових формувань провідних країн. Ключовим етапом у процесі модернізації та оновлення сил безпеки України є формування сучасної системи логістичного забезпечення.

В розрізі розвитку логістичного забезпечення сил безпеки досвід країн з ринковою економікою доводить доречність впровадження державно-приватного партнерства. Таким чином, на сьогоднішньому етапі розвитку демократичного українського суспільства питання управління державно-приватним партнерством постає на передній план. Особливе місце в системі всебічного забезпечення сил безпеки України посідає логістичне забезпечення. Належний рівень логістичного забезпечення сил безпеки в умовах виникнення кризових ситуацій, що загрожують національній безпеці є запорукою ефективного виконання завдань за призначенням.

За таких умов актуальність дослідження обраної теми визначається необхідністю забезпечення належного рівня логістичного забезпеченні сил безпеки України шляхом

запровадження ефективних механізмів управління державно-приватним партнерством.

Теоретичні засади становлення державно-приватного партнерства у складових сектора безпеки і оборони України.

Сьогоднішній розвиток економічної системи України доводить необхідність запровадження дієвих державно управлінських підходів до ефективного забезпечення конкурентоспроможності в умовах виникнення кризових явищ. Умови розширення глобалізаційних процесів визначає, що приватний сектор відіграє важливу роль у забезпеченні соціально-економічного розвитку регіонів держави.

Плани антикризових дій та посткризового відновлення економічної системи держави, що діють в багатьох країнах, передбачають запровадження широкого співробітництва між державою, приватним сектором та громадянським суспільством, які забезпечують дієві механізми державно-приватного партнерства. При цьому, масове розповсюдження принципів державно-приватного партнерства в глобальному просторі відбувається не тільки з причини залученням державних адміністративних структур приватного сектору до виконання суспільно значущих та соціальних завдань соціально-економічного розвитку, а також з метою запровадження інноваційних та ґрунтовних організаційно-управлінських рішень та коштовних виробничих технологій.

Під час посткризового відновлення вітчизняної економіки і становлення конкурентоспроможного соціально-економічного розвитку регіонів та держави в цілому державно-приватне партнерство є прогресивним та ефективним механізмом співробітництва між органами державної влади та місцевого самоврядування, приватним сектором та громадянським суспільством.

Слід зазначити, що наша держава вже мала досвід залучення приватного сектору до розвитку вітчизняної економічної системи. За даними Світового банку, протягом 1990-2011 років за участю приватного сектору реалізовано 40 інфраструктурних проєктів, при цьому загальний обсяг інвестицій у зазначені проекти становив 12,1 млрд. доларів США, з яких близько 90 відсотків були спрямовані на реалізацію проектів у сфері телекомунікацій. В інших країнах з рівнем доходу на одну особу нижче середнього загальний обсяг інвестицій, залучених у 1990-2011 роках для реалізації інфраструктурних проектів за участю приватного сектору, становив 588,5 млрд. доларів США. Ураховуючи те, що до зазначеної категорії належать переважно країни Африки, найменш розвинені країни Південно-Східної Азії та країни СНД, рівень залучення приватного сектору до реалізації інфраструктурних проектів в Україні є незадовільним.

Тому становлення та розвиток державно-приватного партнерства визначається

декількома базовими факторами, що зумовили зростання партнерських форм господарювання в ринковій економіці на відповідних етапах розвитку.

По-перше, одним із найважливіших напрямів лібералізації економіки, курс на яку було взято у більшості країн світу у 1980-х – 1990-х роках, є приватизація національних активів. І тут державно-приватне партнерство зіграло одну з головних ролей.

По-друге, уряди держав не мають у достатніх обсягах фінансових ресурсів, щоб модернізувати, обслуговувати та розширювати інфраструктуру, що перебуває у власності держави. Залучення приватних партнерів до відтворювальних процесів в інфраструктурних галузях держави є вкрай дієвими механізмами.

По-третє, приватні партнери значно більшою мірою, ніж держава володіє мобільністю, швидкістю прийняття рішень, здатністю до нововведень, використання технічних та технологічних змін. Уряд же, в свою чергу, може полегшувати реалізацію проектів шляхом проведення низки інституційних заходів, а також за рахунок фінансово-економічних механізмів, таких як субсидії, гарантії та інші види підтримки.

Класичним фундаментом державно-приватного партнерства є теорія державного регулювання економіки. Складні форми організації та ведення сучасного господарства неможливі без регулювання державою діяльності компаній, галузей та сфер економіки. На підтримку системи економічного регулювання у кожній країні працює значна частина державних інституцій, видається величезне кількість нормативних документів, що модифікуються існуючі та з’являються нові інструменти державно-приватного партнерства, що регламентують дії бізнесу при здійснення різнопланових державно-приватних проєктів.

Відповідно до загального переліку функцій держави в сфері регулювання базовою виступає створення політичних, економічних, правових та інших напрямів для суб’єктів підприємницької діяльності при реалізації ними конкретних проєктів. Отже, у сьогоднішній інституційній формі існування господарського партнерства держави і бізнесу є відносно новий ступінь розвитку теорії державного управління.

Ще однією базовою основою державно-приватного партнерства є теорія громадського сектору економіки. У кожній країні існує потужна, розгалужена система громадського сектору, у межах якого функціонують державно-приватні партнерства. Масштаби громадського сектора у тій чи іншій країні періодично змінюються, що визначається пріоритетами економічної політики, що проводиться, фазою господарського розвитку (зростання, стагнація, рецесія), зовнішньоекономічними умовами та іншими факторами. Роль держави послаблюється в одних і посилюється в інших напрямках. Державно-приватне партнерство у контексті теорії громадського сектора покликане вирішувати завдання

економічного розвитку, удосконалення виробничої інфраструктури, ліквідації та пом'якшення кризових ситуацій соціально-економічного характеру *(Бєлай С. В., 2015).*

В свою чергу, прийняття Закону України «Про державно-приватне партнерство» та відповідних підзаконних актів свідчить про прагнення до широкого впровадження державно-приватного партнерства. Закон регулює договірні відносини держави і приватного сектору у формі концесії, спільної діяльності та інших договорів. У подальшому механізм взаємодії держави і приватного сектору на основних принципах державно-приватного партнерства регулюватиметься спеціальним законодавством, гармонізованим із законодавством ЄС.

Відповідно до Закону «Про державно-приватне партнерство» державно-приватним партнерством є «співробітництво між державою Україна, Автономною Республікою Крим, територіальними громадами в особі відповідних державних органів, які … здійснюють управління об'єктами державної власності, органів місцевого самоврядування, Національною академією наук України, національних галузевих академій наук (державних партнерів) та юридичними особами, крім державних та комунальних підприємств, установ, організацій (приватних партнерів), що здійснюється на основі договору в порядку, встановленому законодавством, та відповідає основним ознакам державно-приватного партнерства».

До основних ознак державно-приватного партнерства законодавець відносить: розбудова (нове будівництво, реконструкція, реставрація, капітальний ремонт та технічне переоснащення) об'єкта державно-приватного партнерства, а також управління (користування, експлуатація, технічне обслуговування) таким об'єктом; довготривалість відносин (встановлено термін від 5 до 50 років); розподіл ризиків у процесі здійснення державно-приватного партнерства; обовязковість інвестування у об'єкти проєктів державно-приватного партнерства.

Розгляд процесів розвитку державно-приватного партнерства в секторі безпеки і оборони потребує більш глибокого вивчення питання функціонування його складових. З цією метою надалі дослідимо це питання.

Відповідно до Закону «Про національну безпеку» під сектором безпеки і оборони України розуміється «система органів державної влади, Збройних Сил України, інших утворених відповідно до законів України військових формувань, правоохоронних та розвідувальних органів, державних органів спеціального призначення з правоохоронними функціями, сил цивільного захисту, оборонно-промислового комплексу України, діяльність яких перебуває під демократичним цивільним контролем і відповідно до Конституції та законів України за функціональним призначенням спрямована на захист національних інтересів України від загроз, а також громадяни та громадські об'єднання, які добровільно

беруть участь у забезпеченні національної безпеки України».

Силами безпеки є «правоохоронні та розвідувальні органи, державні органи спеціального призначення з правоохоронними функціями, сили цивільного захисту та інші органи, на які Конституцією та законами України покладено функції із забезпечення національної безпеки України».

До сил оборони законодавець відносить «Збройні Сили України, а також інші утворені відповідно до законів України військові формування, правоохоронні та розвідувальні органи, органи спеціального призначення з правоохоронними функціями, на які Конституцією та законами України покладено функції із забезпечення оборони держави».

Сектор безпеки і оборони України складається з чотирьох взаємопов'язаних складових: сили безпеки; сили оборони; оборонно-промисловий комплекс; громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки.

Функції та повноваження складових сектору безпеки і оборони визначаються законодавством України.

В розрізі тематики дослідження більш детально розглянемо функції та завдання сил безпеки сектору безпеки і оборони.

Національна поліція України є «центральним органом виконавчої влади, що забезпечує громадську безпеку і порядок, охорону прав і свобод людини, інтересів суспільства і держави, протидію злочинності, а також надає визначені законом послуги з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги».

Завдання поліції є надання поліцейських послуг у сферах: «забезпечення публічної безпеки і порядку; охорони прав і свобод людини, а також інтересів суспільства і держави; протидії злочинності; надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги».

Національна гвардія України є «військовим формуванням з правоохоронними функціями, призначеним для виконання завдань із захисту та охорони життя, прав, свобод і законних інтересів громадян, суспільства і держави від злочинних та інших протиправних посягань, охорони громадського порядку та забезпечення громадської безпеки, а також у взаємодії з іншими органами – із забезпечення державної безпеки і захисту державного кордону України, припинення терористичної діяльності, діяльності незаконних воєнізованих або збройних формувань, організованих злочинних груп та організацій.

Тому у мирний час Національна гвардія України входить до складу сил безпеки сектору

безпеки і оборони України і виконує правоохоронні функції, а також розвиває спроможності, необхідні для виконання завдань у складі сил оборони. Під час запровадження воєнного стану Національна гвардія України приводиться в готовність до виконання завдань за призначенням в умовах дії правового режиму воєнного стану, входить до сил оборони сектору безпеки і оборони України, виконує завдання та підпорядковується відповідно до положень Закону України «Про правовий режим воєнного стану» та Закону України «Про Національну гвардію України».

Далі зупинимось на Державній прикордонній службі України, яка є «правоохоронним органом спеціального призначення, що реалізує державну політику у сфері безпеки державного кордону України та охорони суверенних прав України в її виключній (морській) економічній зоні». Виходячи із функцій Державної прикордонної служби України можливо зазначити, що ця служба входить до складу сил безпеки сектору безпеки і оборони України.

Служба безпеки України є «державним органом спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку, здійснюючи з неухильним дотриманням прав і свобод людини і громадянина: протидію розвідувально-підривній діяльності проти України; боротьбу з тероризмом; контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, інформаційної безпеки держави, об’єктів критичної інфраструктури; охорону державної таємниці». Виходячи із компетенцій і завдань Служби безпеки України можливо зазначити, що ця служба теж входить до складу сил безпеки сектору безпеки і оборони України.

Управління державної охорони України здійснює державну охорону органів державної влади України, забезпечення безпеки посадових осіб та охорони об’єктів. Виходячи із компетенцій і завдань Управління державної охорони України можливо зазначити, що ця служба теж входить до складу сил безпеки сектору безпеки і оборони України.

Державна міграційна служба України є «центральним органом виконавчої влади, що реалізує державну політику у сферах міграції (імміграції та еміграції), зокрема протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, зокрема біженців та інших визначених законодавством категорій мігрантів». Виходячи із завдань Державної міграційної служби України можливо зазначити, що ця служба теж входить до складу сил безпеки сектору безпеки і оборони України.

Державна служба України з надзвичайних ситуацій є «центральним органом виконавчої влади, що реалізує державну політику у сферах цивільного захисту, захисту населення і територій від надзвичайних ситуацій, запобігання їх виникненню, ліквідації

наслідків надзвичайних ситуацій, проведення аварійно-рятувальних робіт, пожежогасіння, пожежної та техногенної безпеки, роботи рятувальних служб під час аварій, а також гідрометеорологічної діяльності». Виходячи із завдань Державної служби України з надзвичайних ситуацій можливо зазначити, що ця служба теж входить до складу сил безпеки сектору безпеки і оборони України.

Таким чином, в розрізі тематики дослідження до сил безпеки сектору безпеки і оборони України доцільно віднести Національну поліцію України, Національну гвардію України, Державну прикордонну службу України, Службу безпеки України, Управління державної охорони України, Державну міграційну службу України, Державну службу України з надзвичайних ситуацій. Надалі в дослідженні під час розгляду основних положень логістичного забезпечення сил безпеки сектору безпеки і оборони України будемо розуміти ці державні органи, служби та військові формування.

У процесі аналізу дослідження виділено такі основні інституційні засади державно-приватного партнерства, що притаманні сфері функціонування сил безпеки сектору безпеки і оборони України та процесу становлення державно-приватного партнерства в Україні.

Принцип рівності та свободи – основний принцип ринкової економіки. Він має два аспекти: по-перше, рівність усіх економічних агентів у доступі до послуг, які надають приватні компанії у сфері державних громадських служб, по-друге, рівність всіх приватних компаній у праві укладання контрактів державно-приватного партнерства. При цьому принципі не допускається соціальна нерівність (за походженням, політичними поглядами) та інші типи дискримінації (за територіальною ознакою, за світоглядом та релігійним переконанням тощо).

Однак принцип рівності та свободи має деякі обмеження, а саме те, що певна частина положень договорів, які укладаються в рамках державно-приватного партнерства, формулюється у відповідності до чинного законодавства і не може служити предметом переговорів сторін. Крім того, цей принцип доповнюється двома протилежними принципами: з одного боку, стабільності контракту державно-приватного партнерства, і, з іншого боку, можливості його зміни, тобто адаптації до умов, що змінилися. Держава або муніципальна освіта, як представник громадської влади та відповідність до принципу адаптації, може в односторонньому порядку і без попередніх консультацій із приватною компанією змінювати умови договору та висувати вимоги, зумовлені наявністю суспільного інтересу (суспільної користі чи блага). При цьому приватна компанія має виконувати свої обов’язки за договором у повному обсязі та з відповідною якістю, навіть якщо вона не погоджується з органом влади. Також вона може оскаржити прийняте державою рішення у судовому порядку.

Принцип безперервності надання послуг. Послуги економічних агентів повинні

забезпечуватися приватною компанією - партнером держави безперервно, що визначається публічно-правовим характером відносин державно-приватного партнерства. Вона за законом не має право припиняти свою роботу. У разі збою у наданні послуги приватна компанія зобов'язана вжити всіх можливих заходів для її відновлення.

Відповідний державний орган, ґрунтуючись на своєму статусі представника влади, може бути в односторонньому порядку і без попередніх консультацій з приватною компанією - оператором змінювати умови договору та висувати вимоги, зумовлені наявністю суспільного інтересу (суспільної користі чи блага). При цьому приватна компанія, навіть якщо вона не згодна з представником держави і збирається оскаржити прийняте ним рішення у судовій інстанції, має, відповідно до законодавства, виконувати свої обов'язки за договором у повному обсязі та з відповідним якістю.

Принцип конкурсності. Як правило, у всіх країнах контракти державно-приватного партнерства видаються за результатами конкурсів. У рідкісних, виняткових випадках, як виняток, а також міркувань національної, державної, економічної, громадської безпеки Держава має право укласти контракти без конкурсу.

Принцип прозорості та зворотного зв'язку. У здійсненні проєктів державно-приватного партнерства держава, громадськість і населення повинні мати доступ до повної інформації про стан підприємства, його фінансові, економічні та інші показниках, якості послуг. Споживачі повинні мати канали зворотний зв'язок з приватними компаніями та державними органами, що контролюють їх роботу.

Принцип невтручання. Держава не має права втручатися в господарсько-адміністративну діяльність приватної компанії після підписання контракту, яка самостійно приймає всі адміністративно-господарські, управлінські, кадрові та інші рішення. Винятком є випадки, що загрожують національним інтересам, перелік яких зазначається додатковими умовами контракту.

Принцип гарантій. Держава застосовує у межах державно-приватного партнерства систему гарантій, обумовлених законом (наприклад, пільговий режим оподаткування). Також з метою реалізації найбільш значущих в сфері безпеки суспільства проєктів держава може надавати їм різноманітну допомогу. Інструментами такої допомоги можуть виступати: дотації з бюджету, державні позики та гарантії по позиках, зниження розміру (скасування) концесійних платежів, орендної плати за землю тощо.

Принцип оплати. Якщо держава в односторонньому порядку або за узгодження з приватною компанією припиняє дію контракту державно-приватного партнерства, то воно має відшкодувати компанії зроблені нею інвестиції та компенсувати недоотриманий їй дохід.

Принцип рівноправного ставлення до іноземних компаній, що забезпечує їм рівні права з вітчизняними компаніями. Вже на стадії розробки основ законодавства щодо державно-приватного партнерства цей принцип втілюється в нормах щодо забезпечення недискримінаційного режиму допуску закордонних компаній до конкурсів з проєктів державно-приватного партнерства, права вільного розпорядження ними чистої прибутком, отриманим на об'єкті державно-приватного партнерства, у тому числі права вивезення чистого прибутку за кордон тощо. Винятком можуть стати випадки, що загрожують функціонуванню силам безпеки, що визнані розвідувально-підривної діяльністю зарубіжних партнерів.

Принцип забезпечення інтересів держави є основоположним базовим принципом, що слугує запобіжником виникнення кризових ситуацій у сфері функціонування сил безпеки сектору безпеки і оборони України. Використання цього принципу є обов'язковим під час запровадження механізмів державно-приватного партнерства.

Таким чином можливо зазначити, що становлення державно-приватного партнерства у складових сектора безпеки України сьогодні знаходиться на етапі започаткування. Наявність різних форм договірних відносин у рамках державно-приватного партнерства регулюються окремими законами та підзаконними актами, що ускладнює формування єдиного підходу до розроблення механізмів впровадження та розвитку державно-приватного партнерства. Також не чітко визначені суб'єкти, які мають право бути державними партнерами у проектах, що реалізуються за участю сил безпеки України, не передбачене застосування механізму інституційного партнерства, можливості для двох і більше органів, служб, військових формувань бути одночасно державними партнерами, заборонена участь державних підприємств у реалізації проєктів державно-приватного партнерства тощо.

Основними проблемами державно-приватного партнерства в сфері забезпечення функціонування сил сектору безпеки сектору безпеки і оборони України є: дефіцит бюджетних коштів та занадто ускладненість реалізації механізмів державної підтримки; відсутність щорічного фінансування довгострокових проєктів державно-приватного партнерства в сфері функціонування сил безпеки; невизначеність методології надання державної підтримки в рамках реалізації проєктів державно-приватного партнерства для сил безпеки; невідповідність принципів і підходів у сфері державно-приватного партнерства існуючим загальноприйнятим міжнародним принципам.

Отже розглянуте свідчить, що для ефективного забезпечення функціонування сил сектору безпеки України, крім удосконалення вітчизняної нормативно-правової бази у сфері державно-приватного партнерства, необхідне застосування механізмів управління державно-

приватним партнерством у логістичному забезпеченні сил безпеки України з метою залучення приватних інвестицій на засадах такого партнерства.

Структура, завдання та функції системи логістичного забезпечення сил безпеки України.

На початку розгляду питання вивчення структури, завдань та функцій системи логістичного забезпечення сил безпеки України дослідимо теоретичні засади термінів логістика та логістичного забезпечення.

Більшість дослідників сходяться на тому, що термін «логістика» започаткувався у Стародавній Греції, де «logistike» означало «рахункове мистецтво» або «мистецтво міркування, обчислення». За часів Римської імперії під логістикою розумілися «правила розподілу продуктів». За часів візантійського імператора Льва VI (866-912 роки) логістика відповідала за забезпечення армії і управління її переміщеннями. Призначенням логістики у Візантійській імперії було «платити платню армії, належним чином озброювати її, забезпечувати зброєю і військовим майном, своєчасно і повною мірою піклуватися про її потреби і, відповідно, готувати кожен акт військового походу», тобто розраховувати простір і час, здійснювати вірний аналіз місцевості з погляду пересування армії, а також сили опору супротивника і відповідно до цих функцій управляти і керувати, одним словом, розпоряджатися рухом і розподілом власних збройних сил.

Автором перших наукових праць з логістики загальновизнано вважати військового діяча А. Жоміні (1779-1869 рр.). В своїх дослідженнях він стверджував, що «логістика охоплює широке коло питань, що включають планування, управління, матеріальне, технічне, продовольче забезпечення військ, а також визначення місця їх дислокації, будівництво доріг, укріплень тощо». Також є твердження, що деякі положення логістики застосовувались в армії Наполеона. Тому існує думка, що поняття «логістика» також має походження від французького слова «loger» (житло, квартира) *(Ларіна Р.Р., 2005)*.

У 1884 р. Американський інститут військово-морського флоту ввів поняття «логістика» для потреб навігації. Широкий розвиток принципи логістики отримали в роки другої світової війни в процесі вирішення завдань матеріально-технічного забезпечення сил безпеки і оборони, дислокованих в Європі, а також організації взаємодії між постачальниками озброєння, продовольства, транспортом і військами.

Отже, як військова наука логістика сформувалась у середині XIX ст. Підходи логістики у військовій справі активно застосовувались в період Другої світової війни. Паралельно з практичним застосуванням в багатьох країнах, перш за все в США і СРСР, розвивається теорія логістики в військовій сфері, яка визначає логістику як науку про планування і управління

переміщенням і матеріально-технічним забезпеченням військ.

Поряд із логістикою у військовій справі існувало також інше трактування терміну. Німецький філософ, математик та фізик В. Лейбніц (1646-1716 рр.) називав логістикою математичну логіку. Таке значення терміну було підтверджено в 1904 р. на філософському конгресі в Женеві.

Отже, історично склались два різних підходи до трактування, а також сфери застосування терміну «логістика», а саме у військовій справі та у математичних розрахунках. Додамо, що із сфери забезпечення військ логістика розширилась на приватну господарську діяльність у формі наукових досліджень щодо управління рухом транспортних потоків.

Вважається, що одним з перших вчених, хто зазначив на можливість використання положень логістики військової сфері в цивільній економіці є професор О. Моргенштерн (США). Він у труді 1951 р. визначив, що є з достатньою долею вірогідності подібність між управлінням забезпечення сил оборони з управлінням матеріальних потоків.

В свою чергу застосування логістики в приватній господарській діяльності та суспільній економіці почалось у шести десяті роки минулого століття. Тому сьогодні логістика розповсюдилась в першу чергу в економічному секторі, але крім того, й у інших сферах, таких, як соціальна, освітня, також культурна та ін. У дев'яностих роках поняття логістика вже отримало дуже широке розповсюдження в різних сферах життєдіяльності суспільства.

Отже, у зарубіжній, а також українській літературі накопичилась велика кількість наукових знань в сфері логістичного забезпечення. Наведені основні суті терміну логістика є практично у всіх європейських мовах. Як вже зазначалось, загальноприйнятого визначення терміну «логістика» як в світі, так і в Україні немає. При цьому розглянемо найбільш поширені сучасні визначення логістики.

У 1974 році пройшов перший Європейський Конгрес з логістики, на якому надано сучасне визначення поняття логістика, як наука про планування, управління та контроль за рухом матеріальних, інформаційних і фінансових ресурсів в різних системах.

В.І. Сергєєв досліджував логістику у двох ракурсах (широкому та вузькому). За широким підходом, логістикою є наука про управління матеріальними потоками, інформацією, що функціонує в ньому, фінансами та сервісом у певній мікро-, мезо- чи макроекономічній системі для досягнення поставлених цілей з оптимальними витратами ресурсів. У вузькому сенсі, а саме з позиції приватних партнерів, логістикою є інструментарій інтегрованого управління матеріальними, інформаційними, фінансовими та ін. потоками, а також супутнім сервісом, якій сприяє досягненню цілей організації бізнесу з оптимальними витратами ресурсів.

Зарубіжними джерелами більш за все розповсюджено визначення логістики як господарської діяльності в приватному секторі, отже процесу управління матеріальними потоками. Теоретичними, методологічними і практичними аспектами розвитку логістики в світі продовжують займатись у США Рада логістичного менеджменту (Council of Logistics Management) та у ЄС – Європейська логістична асоціація (European Logistics Association).

Найбільш розповсюдженим на сьогоднішній час є визначення Ради логістичного менеджменту а саме: «процес планування, виконання і контролю, ефективного з точки зору зниження витрат, потоку запасів сировини, матеріалів, незавершеного виробництва, готової продукції, сервісу і пов'язаної інформації від точки його зародження до точки споживання (включаючи імпорт, експорт, внутрішні та зовнішні переміщення) для повного задоволення вимог споживачів».

В свою чергу, Європейською логістичною асоціацією надано визначення логістики, як «організація, планування, контроль і виконання товарного потоку від проектування і закупівель, через виробництво і розподіл до кінцевого споживача з метою задоволення вимог ринку з мінімальними операційними та капітальними витратами».

Так, в термінологічному словнику: Логістикою (logistics) є «наука про планування, організацію і контроль за транспортуванням, складуванням і іншими матеріальними і нематеріальними операціями, що здійснюються в процесі доведення сировини і матеріалів до виробничого підприємства, внутрізаводської переробки сировини, матеріалів і напівфабрикатів, доведення готової продукції до споживача відповідно до інтересів і вимог останнього, а також передачі, зберігання і обробки відповідної інформації».

Для впровадження логістичних структур та вдосконалення існуючих у приватному секторі бізнес може створювати логістичні центри. Тому розвиток теоретико-методологічних засад логістики реалізується на основі її принципів. Найважливіше значення при розробці і створенні логістичних систем мають принципи, які визначають характер і суть усього устрою узгодження загалом і окремих його аспектів зокрема. Наразі науковою спільнотою розроблено основні принципи, які спрямовують логістичну методологію в приватному секторі.

Принцип синергетичності, який визначає комплексний і системний підхід до досягнення певної мети. Враховуючи взаємодію механізму виробництва і обігу, на базі цього принципу можливо дійти до кращого результату в цілому по структурі за рахунок узгодження дій в усіх взаємопов'язаних логістичних процесах.

Принцип динамічності зазначає, що логістичні процеси повинні відображати суть охоплюваних ними процесів і мають бути динамічними організаціями. Суть логістичного процесу реалізується динамікою, що призводить до економічного розвитку. Тобто

динамічність впроваджується сучасними економічними механізмами розвитку.

Принцип комплектності визнає комплексність логістичних підходів, що складаються за системним підходом комплексом взаємопов'язаних елементів. Отже, незалежна побудова елементів логістичних систем не є придатною. В цих випадках існує достатня вірогідність виникнення кризових ситуацій під час реалізації логістичних потоків.

Принцип ініціативності визнає, що логістичні системи та відповідні процеси базуються на ініціативних суб'єктивних умовах, що дуже позитивно впливають та визначають основи розвитку соціально-економічних систем та процесів.

Принцип доцільності орієнтується на залученні ефективного базису, що визначає головну роль у логістичному забезпечені. Під час обґрунтування організаційно-технологічних механізмів головним завданням виступає підвищення ефективності, а саме кількості витрат або часу на переміщення товаропотоку враховуючи форс-мажорні обставини.

Отже, в цілому за наданими класичним визначеннями логістичне управління відповідає на наступні питання: що саме і в якому об'ємі слід виготовляти власними силами, а що купувати у постачальників; як розмістити замовлення і спланувати складську мережу; як здійснювати вибір устаткування; як здійснювати планування; як здійснювати вибір структури і реалізацію внутрішньої транспортної системи і управляти її функціонуванням; як здійснювати диспетчеризацію і виробничий контроль; як створити ефективну систему складування; як здійснювати облік і управління запасами готової продукції. Таким чином, глобальним (головним) завданням в логістиці є – досягнення максимального ефекту з мінімумом витрат в умовах не стабільної обстановки на ринку. До глобальних завдань відносять також моделювання логістичних систем і умов їх надійного функціонування.

Виходячи з тематики дослідження, надалі розглянемо зміст терміну логістики в військовій справі.

Сьогодні концептуально вводиться нове поняття «логістика» (відповідно до STANAG 2406 – «Доктрина з матеріально-технічного забезпечення Сухопутних військ НАТО»), як наука з планування й здійснення переміщення та забезпечення військ (сил), яка застосовується до аспектів військових операцій, пов'язаних із такими видами діяльності: проектування, розробка (модернізація та модифікація), закупівля, зберігання, транспортування, розподіл, технічне обслуговування та ремонт, евакуація та утилізація матеріально-технічних засобів; транспортування особового складу; закупівля або будівництво, технічне обслуговування, експлуатація та реалізація військових об'єктів; закупівля або надання послуг із харчування, лазне-прального обслуговування тощо; медичне забезпечення.

Логістичне забезпечення – це комплекс взаємопов'язаних заходів, який забезпечує

діяльність сил безпеки у мирний та воєнний час. Логістичне забезпечення включає: планування логістичного забезпечення, визначення потреб у матеріально-технічних засобів, проєктування, розроблення (модернізацію та модифікацію) озброєння, військової техніки та матеріально-технічних засобів, їх закупівлю, постачання, зберігання, ремонт, технічне обслуговування, контроль експлуатації (використання), реалізації, списання та утилізації надлишкового озброєння, спеціальної техніки та матеріально-технічних засобів, планування та здійснення військових перевезень усіма видами транспорту, розквартирування сил, закупівлю робіт та послуг, лазне-пральне та торговельно-побутове обслуговування, організацію харчування, закупівлю або будівництво, технічне обслуговування, експлуатацію об'єктів військової інфраструктури.

Таким чином, система логістики – це сукупність органів управління логістикою, сил і засобів логістичного забезпечення, призначених для виконання завдань логістичного забезпечення сил безпеки сектору безпеки і оборони України, між якими існують зв'язок та взаємодія. Систему логістики сил безпеки доречно поділити на загальнодержавний, регіональний та місцеві рівні, між якими існує чіткий розподіл функцій та повноважень щодо організації логістичного забезпечення сил безпеки сектору безпеки і оборони України. Структурно система логістики сил безпеки сектору безпеки і оборони України повинна включати: на загальнодержавному рівні – структурні підрозділи Міністерства внутрішніх справ України, Служби безпеки України, Управління державної охорони України із завданням щодо організації проєктування, розробки (модернізації та модифікації), закупівлі і постачання озброєння та спеціальної техніки, матеріально-технічних засобів, надання послуг та їх фінансування в обсягах, необхідних для ефективного виконання силами безпеки покладених на них завдань; на регіональному рівні – управління логістики та подібних органів управління Національної поліції України, Національної гвардії України, Державної прикордонної служби України, Служби безпеки України, Управління державної охорони України, Державної міграційної служби України, Державної служби України з надзвичайних ситуацій з підпорядкованими силами та засобами логістичного забезпечення із завданнями щодо планування та організації логістичного забезпечення сил безпеки у їх повсякденній діяльності, під час проведення заходів підготовки, відмобілізування, підготовки та ведення спеціальних операцій тощо; на місцевому рівні – відділи логістики та подібних структур органів та підрозділів сил сектору безпеки сектору безпеки і оборони України з підпорядкованими засобами логістичного забезпечення, призначені для вирішення завдань логістичного забезпечення у їх повсякденній діяльності, під час заходів підготовки, виконання завдань за призначенням.

Отже, плануванням логістичного забезпечення є комплекс заходів щодо визначення завдань логістичного забезпечення, порядку управління системою логістики, обсягів озброєння та спеціальної техніки, матеріально-технічних засобів та порядку їх підвозу і поповнення, послідовності, термінів, способів дій, взаємодії, необхідного складу угруповань сил і засобів логістики, розроблення відповідних планувальних документів для виконання завдань із забезпечення сил безпеки у мирний, під час виникнення кризових ситуацій та особливий період.

Під час планування логістичного забезпечення сил безпеки сектору безпеки і оборони України повинні визначатися: мета, основні завдання та напрями зосередження основних зусиль логістичного забезпечення сил безпеки; сили та засоби логістичного забезпечення; потреба та порядок забезпечення озброєння та спеціальної техніки, матеріально-технічних засобів; порядок створення, утримання, поповнення та використання запасів матеріально-технічних засобів; порядок проведення технічного обслуговування та відновлення озброєння та спеціальної техніки, інших технічних засобів; напрями нарощування спроможностей логістичного забезпечення; порядок використання можливостей складових національної економіки держави для виконання завдань логістичного забезпечення сил безпеки; порядок управління та взаємодії під час виконання завдань з логістичного забезпечення.

Надалі розглянемо функції логістичного забезпечення сил безпеки сектору безпеки і оборони України, основними з яких є: постачання та обслуговування; технічне обслуговування та ремонт; перевезення та транспортування; інженерно-інфраструктурне забезпечення; здійснення закупівель та постачання товарів, робіт і послуг для забезпечення потреб сил безпеки; делегування повноважень; аудит та інспекція; підготовка та навчання; стандартизація у сфері логістичного забезпечення; управління інформацією логістичного забезпечення (інформаційної логістики).

Функція технічного обслуговування та ремонту спрямована на підтримання озброєння та спеціальної техніки в готовності до застосування, виконання заходів щодо евакуації озброєння та спеціальної техніки з експлуатаційними пошкодженнями, відновлення справності (технічної придатності) озброєння та спеціальної техніки шляхом проведення відповідних видів ремонту, відновлення та подовження їх ресурсу.

Функція перевезення та транспортування включає в себе повний спектр організацій, інфраструктури, обладнання та технічних засобів, необхідних для забезпечення розгортання сил безпеки та ведення ними спеціальних операцій та виконання завдань за призначенням. Перевезення та транспортування полягає у проведенні своєчасного планування та організації перевезення сил, підвезенні (подачі) озброєння та спеціальної техніки, матеріально-технічних

засобів та їх евакуації всіма видами транспорту, підготовки і розподілу транспортних засобів, розгортанні транспортних комунікацій для виконання визначених завдань.

Функція інженерно-інфраструктурного забезпечення охоплює комплекс заходів з утримання інфраструктури логістичного забезпечення сил безпеки як стаціонарної, так і мобільної, виконання заходів їх живучості. Вона включає: закупівлю, оренду, утримання та удосконалення об'єктів для зберігання матеріально-технічних засобів, проведення технічного обслуговування і ремонту озброєння та спеціальної техніки, розміщення особового складу (у польових умовах – розгортання в місцях розташування військових частин (підрозділів) оперативних баз (польових таборів, польових складів, польових ремонтних майстерень), їх обладнання мережами енергопостачання, обігріву, водопостачання та каналізації (утилізації відходів життєдіяльності), системою охорони та оборони, під'їзними шляхами; організацію їх експлуатації та підтримання в робочому стані тощо; створення необхідних житлово-побутових умов для особового складу як у стаціонарних, так і польових умовах; сприяння прийманню, зосередженню та подальшому висуванню сил; відновлення та технічне обслуговування комунікацій, сприяння захисту зовнішнього середовища.

Закупівлі повинні бути зорієнтовані на забезпечення найбільш економічно вигідної пропозиції щодо всього життєвого циклу озброєння та спеціальної техніки, матеріально-технічних засобів та інших предметів постачання. Закупівля товарів, робіт і послуг, що підлягають закупівлі відповідно до угод, що укладаються зі спеціалізованими організаціями здійснюється згідно з правилами і процедурами, установленими відповідними спеціалізованими організаціями. Процедури публічних закупівель повинні бути зорієнтовані на встановлення довготривалих та прогнозних контрактів (рамкових угод) з підприємствами національної та міжнародної економіки, досягнення максимального ефекту економії, прогнозування забезпечення та якості забезпечення.

Для забезпечення ефективного функціонування системи логістики сил безпеки, а також свободи маневру для керівників органів управління логістики на всіх рівнях передбачається впровадження системи делегування повноважень відповідно до таких принципів: повноваження делегуються від керівної (вищої) посади до підлеглої (нижчої); перед делегуванням повинен бути проведений аналіз можливих ризиків; внаслідок делегування відповідальності особа, яка делегувала, не звільняється від відповідальності; делегування передбачає чіткий перелік повноважень, які передаються підлеглому. До повноважень, які підлягають делегуванню відносяться: право підпису та право прийняття рішень; право укладання договорів розпорядниками коштів відповідного ступеня; право прийняття рішення щодо переміщення запасів матеріально-технічних засобів, з метою їх наближення до органів

та підрозділів сил безпеки.

Перевірка, яка необхідна для функціонування будь-якої системи логістики, як правило, поділяється на два рівні: інспекція оперативних стандартів; аудит технічних і нормативних стандартів. Інспекція оперативних стандартів – це перевірка боєздатності органів управління логістикою, сил та засобів логістичного забезпечення. Така інспекція повинна проводитися керівником органу управління. Аудит здійснює оцінку системи управління (корпоративного управління), внутрішнього контролю та управління ризиками з метою надання вищому керівництву та керівникам об'єктивних і незалежних висновків, рекомендацій та пропозицій щодо: функціонування системи внутрішнього контролю та її удосконалення; удосконалення системи управління; запобігання фактам незаконного, неефективного та не результативного використання фінансового, матеріальних та інших ресурсів; запобігання виникненню помилок чи інших недоліків.

З метою підтримання спроможностей органів управління логістикою, сил та засобів логістичного забезпечення до виконання завдань за призначенням з ними проводяться відповідні заходи професійної підготовки. Підготовка органів управління логістикою, сил та засобів логістичного забезпечення включає збалансоване поєднання теорії та практики. Ключовими аспектами підготовки є: відповідність підготовки органів управління та підрозділів логістики завданням, визначеним у планах їх застосування, з наданням пріоритету їх практичній підготовці, яка базується на стандартах ЄС та НАТО; обґрунтованість процесу підготовки та його змісту, з урахуванням останніх досягнень науки і техніки; системний підхід до розподілу змісту підготовки за періодами підготовки (строками навчання), тісний взаємозв'язок та наступність підготовки, відповідність вимогам оперативним стандартам підготовки; системне використання різних форм і методів підготовки для формування в тих, хто навчається, визначених фахових здібностей за стандартами підготовки для виконання обов'язків за посадою (спеціальністю); відповідність змісту, форм і методів навчання рівню підготовки особового складу.

Стандартизація у сфері логістичного забезпечення в залежності від об'єкта стандартизації поділяється на адміністративну та оперативну і матеріальну складові та являє собою діяльність, що полягає в установленні положень для загального і багаторазового застосування щодо концептуальних, програмних та нормативних документів (проєктів), спрямованих на досягнення та підтримку взаємосумісності сил безпеки сектору безпеки і оборони України, а також сил безпеки – країн ЄС та членів НАТО, здатності до взаємодії, взаємозамінності та уніфікації озброєння та спеціальної техніки та інших предметів постачання, підвищення ефективності процедур логістичного забезпечення. Завданнями

стандартизації є: визначення вимог до процесів та процедур логістичного забезпечення; підвищення ефективності та результативності процесів логістичного забезпечення; постійне вдосконалення процесів логістичного забезпечення; підвищення якості, бойових можливостей та ефективності застосування озброєння та спеціальної техніки та інших предметів постачання; скорочення термінів та витрат на розробку, виробництво і ремонт озброєння та спеціальної техніки та інших предметів постачання, номенклатури її складових частин та комплектуючих виробів; покращення показників сумісності та взаємозамінності зразків озброєння та спеціальної техніки та інших предметів постачання, їх складових частин; досягнення максимальної економії при спільному використанні ресурсів і результатів наукових досліджень.

Функція управління інформацією в ході логістичного забезпечення (інформаційна логістика) – діяльність, що забезпечує своєчасне надання керівництву, управлінській ланці та виконавцям інформації для своєчасного прийняття управлінських рішень. Функції управління інформацією логістичного забезпечення сил безпеки повинні бути автоматизовані за допомогою відповідних автоматизованих (інформаційних) систем, що реалізують функції автоматизації: документообігу, бюджетних процесів, закупівель та укладання договорів, отримання, видачі, обліку матеріально-технічних засобів, наявності запасів, надлишку майна, списання, витрачання, передачі матеріально-технічних засобів, стандартизації та кодифікації у сфері логістичного забезпечення, контролю та управління.

Таким чином досліджені теоретичні засади термінів логістика та логістичного забезпечення довели, що найважливіше значення при розробці і створенні логістичних систем мають принципи логістичного забезпечення. Систему логістики сил безпеки доречно поділити на загальнодержавний, регіональний та місцеві рівні, між якими існує чіткий розподіл функцій та повноважень щодо організації логістичного забезпечення сил безпеки сектору безпеки і оборони України. Функції логістичного забезпечення сил безпеки сектору безпеки і оборони України в свою чергу розкривають зміст організації логістичного забезпечення.

Роль і місце державного управління державно-приватним партнерством у логістичному забезпеченні сил безпеки України.

Сьогоднішній розвиток нашої держави постійно супроводжується виникненням кризових ситуацій, що загрожують державній безпеці. Незворотна глобалізація зближує Україну з ЄС. При цьому, Російська Федерація не готова прийняти євроінтеграцію України, як підсумок – збройна агресія у Донецькій та Луганській областях, а також загроза широкомасштабного вторгнення ворожих військ на всю територію України. Крім того, в умовах збройного протистояння й на іншій території України виникають кризові ситуацій.

Зазначені події стали поштовхом для масштабних і структурних реформ у сфері безпеки України. Головним напрямом цього руху є поступове реформування сил сектору безпеки відповідно до стандартів ЄС та НАТО. Тому наразі військові формування та правоохоронні органи спеціального призначення України рухаються шляхом реформування та розбудови за зразком безпекових формувань провідних країн ЄС та НАТО. Ключовим етапом у процесі модернізації та оновлення сил безпеки України є формування сучасної системи логістичного забезпечення.

В розрізі розвитку логістичного забезпечення сил безпеки досвід країн з ринкової економікою доводе доречність впровадження державно-приватного партнерства. Таким чином, на сьогоднішньому етапі становлення демократичного Українського суспільства питання управління державно-приватним партнерством переходе на передній план. Особливе місце в системі всебічного забезпечення сил безпеки України посідає логістичне забезпечення. Належний рівень логістичного забезпечення сил безпеки в умовах виникнення кризових ситуацій, що загрожують державній безпеці є запорукою ефективного виконання завдань за призначенням.

Світовий досвід актуалізує питання розвитку державно-приватного партнерства в сучасних державах з ринковою економікою. Наразі є безліч позивних прикладів становлення міцної економіки за рахунок реалізації механізмів співпраці держави та громадянського сектору, впровадження інноваційних підходів у розвиток державних інституцій.

Тісні зв’язки між державою та підприємницьким сектором випливають із самої сутності ринкової системи управління та правої держави. В ефективній ринковій економіці держава та бізнес, образно кажучи, «йдуть рука об руку».

Концепція державно-приватного партнерства визначається природою держави, щодо якої наукова спільнота має дві основні точки зору. Перша з них акцентує увагу на поданні держави як інструменту для реалізації інтересів бізнес-спільноти, друга – визначає нейтралітет держави стосовно бізнесу та віддає пріоритет інтересам всього суспільства. У руслі такого розуміння сутності держави одні стверджують, що державно-приватне партнерство є апаратом, який створений державою та відповідає інтересам бізнесу, а інші заявляють, що партнерство є механізмом, що відбиває інтереси широкого діапазону класів та громадських груп *(Milliband R., 1974).*

Низька науковців досить категоричні у своїй думці щодо явного зближення державно-приватного партнерства у бік обслуговування інтересів капіталу. Ті вчені як Т. Барнеков, Р. Бойл та Д. Річ доводять, що державно-приватне партнерство – це свого роду механізм, з якого держава обслуговує капітал *(Barnekov T., Boyle R. and Rich D., 1989).* Багато дослідження

показують, як органи державної влади допомагають приватному капіталу максимізувати прибуток від проєктів у рамках партнерства з державою. Внаслідок проведеного аналізу діяльності державно-приватного партнерства у сфері міського розвитку в США, дослідники зазначають, що головною їх метою було створення умов для розвитку великих корпорацій та великої промисловості. Таких висновків дійшов також японський вчений З. Кітаджіма *(JP 4-02, 2012).*

У той же час інші дослідники вважають, що державно-приватне партнерство є механізмом, що сприяє гармонійному розвитку економіки та впливає на користь всього товариства. Так, Ф. Кук доводить, що державно-приватне партнерство для органів місцевого самоврядування можуть бути засобом для здійснення ними прогресивної політики. Мейєр не виключає того, що державно-приватне партнерство є інтересами окремих груп. В теж час вона вважає, що державно-приватне партнерства є також інструментом розвитку в інтересах різних класів та груп суспільства, оскільки вони реалізують реальні проєкти та реалізуються органами державної влади спільно з приватними компаніями на користь суспільству.

У поєднанні держави та бізнесу в одному союзі проявляється суперечність між обслуговуванням суспільних інтересів та забезпеченням прибутку. Виникає ряд запитань, а саме: яким чином державно-приватне партнерство вирішує зазначене протиріччя?, як воно впливає на соціально-економічні відносини в країні, регіоні, місті?, які соціально-економічні будуть у суспільстві в результаті передачі приватному сектору видів виробництв та послуг, що традиційно належать до сфер державної діяльності? Відповіді на всі ці запитання залежать від ступеня зрілості цивільного суспільства, органів державної влади, розвиненості громадських інститутів контролю за діяльністю державного апарату, прозорості самої партнерської діяльності.

Навіть у розвинених країнах з потужною інституційною базою партнерських відносин державно-приватне партнерство часто використовується для реалізації переважно приватного інтересу. Подібні негативні прояви та спотворення суті партнерських відносин призводять до появи деформацій в економічній політиці, порушення умов конкуренції, зростання недовіри до самого феномена партнерських відносин між державою та приватним сектором. Насправді ці явища часто набувають різноманітних форм корупції.

У повсякденній свідомості головна відмінність інститутів ринку та держави полягає в тому, що ринок являє собою сукупність хаотичних (спонтанних) угод купівлі-продажу, а держава виступає у цьому процесі головною регулюючою та стабілізуючою силою. Однак це спрощення реальної дійсності. Є безліч прикладів, коли надмірне втручання держави позначається деструктивно на економічному розвитку, а посилення регулювання гальмує

економічне зростання та науково-технічний прогрес.

Інституційною основою державного втручання в економіку служить виконання ним функцій щодо забезпечення прав власності, створення можливостей для вільної конкуренції та рівного доступу всіх економічних суб'єктів до суспільних благ, а також обмеження доступу до деяких ресурсів. При цьому головним критерієм має виступати суспільний інтерес, виражений у якійсь інтегральній формі, а не вигода окремих суб'єктів господарської діяльності.

Іншими словами, державне втручання має бути націлене, насамперед, на ліквідацію провалів ринку, які виражаються, зокрема, у монополії, в недостатній прибутковості окремих видів діяльності, структурних диспропорціях та інших кризових явищах соціально-економічного характеру.

Зазначені недоліки ринкового механізму найбільш наочно виявляються саме в галузях виробничої та соціальної інфраструктури, які відіграють важливу роль в економіці, а також у науково-технічній галузі, де роль держави завжди була і залишається традиційно сильною, різнобічною і об'єктивно обумовленою.

До того ж, сучасне партнерство держави та приватного сектору, по суті, є непрямою або частковою приватизацією. Деякі вчені процес створення партнерств називають навіть просто приватизацією. Так, у фундаментальному американському дослідженні «Партнерство держави та приватного сектору: фінансування суспільного добробуту» говориться, що одним із альтернативних джерел фінансування витрат на інфраструктуру може бути приватизація, тобто різні угоди відповідно до яких значно зростає участь приватних компаній у фінансуванні, проєктуванні, будівництві, володінні та експлуатації державних підприємств».

При цього є й інша думка, що державно-приватне партнерство – це взагалі приватизація. М.Б. Джеррард зазначає, що партнерства створюються та діють на кордоні державного та приватного секторів господарства, не будучи, водночас, ні націоналізованими, ні приватизованими активами та послугами. Таким чином, політично, вони являють собою третій шлях, за допомогою якого уряди можуть надавати населенню деякі громадські послуги.

Якщо чиста приватизація означає вихід держави з економіки, її окремих сфер і виробництв, створення партнерств призводить лише до передачі частини економічних, організаційних, управлінських функцій щодо державних об'єктів бізнесу. Але самі об'єкти залишаються незмінно в власності держави. На відміну від чистої приватизації у вигляді партнерств держава демонструє свою господарську активність. Діяльність державно-приватного партнерства розглядається як прояв державного втручання та контролю над економічними процесами. Економічно такі партнерства означають систему інституційних

перетворень державного сектору економіки. Вони є реформуванням щодо ведення державою видів та сфер діяльності на шляхах часткової (або відносної) приватизації.

Західна економічна теорія застосовує до наданих на концесійній та іншій партнерській основі послуг у сферах виробничої інфраструктури та природних монополій поняття «приватний товар». Для того щоб приватні компанії, що функціонують у цих сферах, досягали своїх цілей, має бути виконано дві умови. По-перше, вони повинні мати право виключати з обслуговування тих партнерів, які не бажають оплачувати послугу. По-друге, має виконуватися умова конкуренції, тобто надавачі послуг не мають права обмежувати вибір кожним користувачем альтернативних постачальників.

Виконання цих умов покликане гарантувати, що новий регульований державою режим державно-приватного партнерства у сфері логістичного забезпечення сил безпеки, як альтернативи приватизації, дозволить суспільству загалом відчути видимі вигоди таких напівприватизаційних реформ державної власності.

Система партнерських відносин, що склалися до теперішнього часу держави з приватним сектором є одним із елементів змішаної економіки. Необхідність її створення випливає із двох постулатів ліберальної концепції розвитку: по-перше, відповідності між формуванням інститутів сучасної приватної власності та процесом прискорення економічного зростання та по-друге, вищої продуктивності та ефективності економіки, заснованої на приватної власності, порівняно з господарством, що базується на державній власності та прямому державну управління.

Економічний ефект як для суспільства в цілому, так і для сил безпеки сектору безпеки і оборони України полягає в тому, що вони отримують більш якісні товари та високий рівень обслуговування за більш низьких витрат.

Форми реалізації державно-приватного партнерства можуть бути самими різноманітними. У деяких випадках органи влади організують спільне з бізнес-підприємство або підписують з приватною компанією контракт на здійснення проекту. Іноді вони створюють спеціальні фіскальні, податкові, митні режими та механізми регулювання для проєктів державно-приватного партнерства, що пов’язано із внесенням змін до законодавчих та нормативних правових актів.

У зарубіжній та вітчизняній літературі існує безліч класифікацій різновидів, форм, типів та видів партнерств держави та бізнесу у господарській сфері. Як критерії віднесення до тієї чи іншої структурної групи зазвичай виступають: відносини власності (володіння, користування), ступінь залежності від держави, насамперед у питаннях фінансування та поділу ризиків та інші параметри. Але практично у всіх класифікаціях першому місці стоять

концесії.

Слово «концесія» походить від латинського concessio – дозвіл (англ. concession) і означає поступку, угоду, послаблення, знижку. Воно відноситься до економічним категоріям, які мають безліч різних трактувань, позбавлені термінологічної та смислової чіткості та охоплюють широке коло об'єктів. У концесію може передаватися підприємство, вид діяльності, право на надання послуги. Іноді під концесією розуміється сам концесійний договір. Концесія як поняття не має предметної визначеності, оскільки сфера його застосування надзвичайно широке. Наукова спільнота зазначає, що термін концесія є один із самих розпливчастих термінів у адміністративному праві. Його використовують для позначення операцій, що мають дуже мало спільного, якщо не вважати, що в них основі лежить дозвіл, виданий адміністрацією.

Особливу та зростаючу роль ця форма господарювання починає грати у галузях виробничої інфраструктури, що становлять основу систем життєзабезпечення економіки та суспільства та традиційно перебувають у державної власності: електроенергетики, залізничного транспорту, автодорожньому господарстві, портах, аеропортах, магістральному транспортуванні газу, комунальному господарстві тощо. Поширення концесій на нові сфери та удосконалення їх господарського механізму, що відбувається при цьому є головною характерною рисою розвитку концесій у сьогоднішній час.

Концесії є найбільш розвиненою, прогресивною та комплексною формою державно-приватного партнерства. Концесії, на відміну контрактних відносин, мають довгостроковий характер, що дозволяє державним та приватним партнерам реалізовувати стратегічне планування. Крім того, у концесіях приватний сектор має повну свободу у прийнятті адміністративних, господарських та управлінських рішень, що відрізняє їхню відмінність від змішаних підприємств. Також, у держави у рамках концесійного договору, і публічно-правових норм загалом залишається досить важелів на приватного партнера якщо ним порушені умови концесії чи законодавства, а також для захисту інтересів.

Водночас концесіям як формі господарювання притаманні і недоліки, які характерні інших форм партнерства. В основному вони пов’язані з тим, що у договорах концесії, що надаються на тривалі терміни не можуть бути передбачені всі можливі події. Фіксування системи відносин держави та бізнесу на тривалу перспективу, детермінованість багатьох закладених у концесійному договорі положень призводять до відсутності гнучкості та динамічності, характерної для сучасної економіки. Інший недолік концесій полягає в тому, що об’єкти інфраструктури мають тривалі терміни окупності та повернення інвестицій. Складнощі проведення довгострокових фінансово-економічних розрахунків щодо такого роду

об’єктам викликають неточності і навіть помилки, що призводить до додаткових ризиків невиконання умов концесій.

Другою основною форму реалізації державно-приватного партнерства є контракти. Контракти на закупівлю товарів для державних потреб та надання від імені уряди послуг у сфері виробничої інфраструктури припускають отримання приватною компанією – партнером держави компенсації у вигляді частки доходу, прибутку чи платежів. Часто контракти мають форму договорів підряду. Характерною особливістю державних контрактів є їх адміністративна природа, а також те, що права власності на предмет контрактних відносин не передаються державою приватному підприємцю.

Сьогодні контрактна форма партнерських відносин держави та бізнесу має дуже широке поширення у світі. Так, у США федеральне уряд розміщує щорічно від 13 до 15 млн. контрактів на всі види товарів та послуг військового та цивільного призначення. Отримання федерального контракту розцінюється будь-якою приватною компанією як дуже привабливий і престижний бізнес, оскільки він не тільки гарантує певний ринок та дохід, але і є джерелом інших, дуже різноманітних пільг та преференцій.

Для державно-приватного партнерства притаманною є ще одна форма реалізації – угода про розподіл продукції, яка є самостійною формою партнерських відносин держави та приватного сектору, близької, але не відносяться до традиційної концесії. За угодами про розподіл продукції партнеру держави належить лише частина виробленої продукції, а в концесіях же концесіонер є власником усієї випущеної продукції. Навіть якщо, у відповідності до концесійного договору, держава отримує частину податків та інших платежів, наприклад, концесійних, у натуральному вигляді, то це не розділ продукції, а лише заміна однієї форми розрахунків іншою, більш зручною, що влаштовує обидві сторони.

Орендні відносини теж є формою реалізації державно-приватного партнерства. Законодавець виділяє три правомочності права власника: володіння, користування та розпорядження своїм майном. Оренда передбачає передачу на певних умовах приватному сектору державного або муніципального майна (землі, обладнання, приміщення тощо) у тимчасове користування за певну плату на основі орендного договору.

Лізинг є формою близькою до оренди – є як вид інвестиційної діяльності з придбання майна та передачі його на підставі договору лізингу фізичним чи юридичним особам за певну плату, на певний термін та на певних умовах, обумовлених договором, з правом викупу майна лізинг одержувачем.

Можливо зробити висновок, що на відміну від оренди та лізингу в концесіях приватний підприємець та держава перебувають у більш складних та багатоаспектних відносинах.

Відмінності оренди (лізингу) та концесії у тією чи іншою мірою стосуються практично всіх аспектів і характеристик: цілі, предмета, об'єктів, контролю та нагляду, складу контролюючих органів тощо.

Визначення складу проєктів державно-приватного партнерства, їх масштабів та меж є прерогативою держави і залежить від багатьох специфічних для кожної галузі факторів, особливого для логістичного забезпечення сил безпеки сектору безпеки і оборони України. Таким чином, одна із закономірностей формування та розвитку сучасної системи державно-приватного партнерства полягає у реалізації з боку держави комплексних міжгалузевих проєктів партнерства, найчастіше – концесій та контрактів. У сфері логістичного забезпечення сил безпеки більшою мірою розповсюдженні контракти.

Невід'ємною частиною систем партнерства держави та бізнесу є методи державного регулювання. Держава формує інституційне середовище партнерств, займається питаннями організації та управління процесом державно-приватного партнерства, виробляє стратегію та принципи, на яких будуються відносини бізнесу з владою та суспільством у рамках партнерських проєктів. Держава отримує концесійні платежі, контролює ціни, доходи, якість послуг, виконання приватним партнером закріплених у договорі обов'язків. Крім того, держава виробляє тарифну та митну політику, що стимулюють приватну діяльність на об'єктах державної власності та зазвичай субсидуються із бюджету. Водночас важелі державного регулювання застосовуються вибірково, залежно від галузі, типу партнерства, соціальної значущості проєктів та інших чинників особливо у сфері логістичного забезпечення сил безпеки сектору безпеки і оборони України.

Таким чином, реалізація механізмів державно-приватного партнерства дозволяє державі: при збереженні об'єкта у громадській власності передавати його у володіння та користування приватним сектором на поворотній основі при дотримання суворого контролю над діяльністю приватної компанії; перекласти функції будівництва, експлуатації, утримання об'єктів громадської власності, насамперед у сфері виробничої та соціальної інфраструктури, на приватний сектор; забезпечити технічний та технологічний розвиток державних та муніципальних виробництв, об'єктів та послуг; створити умови та передумови для ефективного функціонування виробничих об'єктів, які перебувають у громадській власності, оптимального управління ними, раціональної експлуатації природних ресурсів, захисту довкілля; переривати дію контракту у разі порушення приватною компанією його умов та положень, повертати об'єкт у державне управління або передавати його іншому суб'єкту господарювання; більш повно реалізовувати принципи соціальної справедливості при оптимізації державного втручання у економіку; забезпечувати реальне партнерство держави

та приватного сектору на пріоритетні напрями реформування; формувати конкурентні ринки у сфері окремих сегментів державної та муніципальної власності; отримувати додаткові платежі до бюджетів усіх рівнів.

Держава відмовляється від неефективних форм господарювання, перекладаючи функції управління належною йому власністю на приватний сектор, який, у свою чергу, користуючись державними гарантіями, привносить у виробництво організаційний досвід, знання, ноу-хау, здійснює інвестиції, що мінімізує ризики підприємницької діяльності.

При цьому додамо, що державно-приватне партнерство застосовується з урахуванням особливостей правового режиму щодо окремих об'єктів та окремих видів діяльності, встановлених законом. Тому процес прийняття рішення щодо застосування механізмів державно-приватного партнерства в сфері безпеки держави є занадто складний та не позбавлений корупційної складової.

Реалізація завдань держави у сфері безпеки є базовою функцією, що містить елементи високої складності та має характер динамічності та невизначеності. Поєднання ресурсів державного та приватного сектору надає нових можливостей щодо забезпечення важливих чинників безпеки. Тому з позиції сучасних наукових поглядів державно-приватне партнерство визначене як сучасний механізм співпраці у сфері безпеки. Враховуючи управлінську оперативність, технічний та фаховий потенціал, залучення власних інвестицій, приватний сектор має можливість вирішувати делеговані державою завдання щодо протидії актуальним загрозам державній безпеці.

Наукова спільнота вбачає за нагальну потребу розвитку державно-приватного партнерства у сфері забезпечення безпеки стратегічної інфраструктури. Він зазначає на необхідність ухвалення базового закону, який має врахувати особливості і специфіку функціонування та стану окремих систем (секторів) стратегічної інфраструктури та їх безпеки, а також на впровадження досвіду провідних країн світу і на перспективу входження України до загальноєвропейської безпекової системи. Автор впевнений, що це дасть змогу чітко визначити критерії й методологію віднесення тих чи інших об'єктів національної інфраструктури до стратегічної інфраструктури із подальшою градацією на життєво важливі, важливі і необхідні, а також запровадити комплексний підхід до забезпечення їх безпеки та уніфікувати термінологію у цій сфері. Крім того автори наголошують на розроблення низки підзаконних актів з питань публічно-приватної взаємодії та партнерства, особливостей залучення приватного партнера, процедур, умов, порядку, форм здійснення, прийняття рішення про здійснення такого партнерства.

Продовжуючи питання захисту об'єктів критичної інфраструктури зупинимось на

відповідному дослідженні. Основними принципами функціонування національної системи захисту критичної інфраструктури, якими є: єдність методологічних засад; координованість; державно-приватне партнерство; безпека, захист та охорона інформації з обмеженим доступом; міжнародне співробітництво. Отже бачимо, що державно-приватне партнерство зазначено окремим принципом. Така позиціє є новітньою, так як в законодавчих та нормативно-правових актах сфери функціонування сил безпеки України питання державно-приватного партнерства майже не піднімається. Тому вбачаємо, що цей проєкт є сучасним й перспективним щодо розвитку державно-приватного партнерства в секторі безпеки і оборони України.

Аналіз нормативно-правових джерел, наукових досліджень та практики впровадження державно-приватного партнерства в Україні засвідчує, що ця сфера знаходиться започаткованому стані. Наразі державно-приватне партнерство розвинене в основному у державному (муніципальному) секторі, а саме в житлово-комунальному господарстві, транспорті та медицині. При цьому поза увагою залишаються питання розвитку у сфері забезпечення державної безпеки. В цьому аспекті додамо, що впровадження ефективних механізмів реагування на кризові ситуації, що загрожують державній безпеці є неможливим без сучасного логістичного забезпечення сил безпеки, що включає комплекс заходів щодо своєчасного і повного витребування, отримання та створення запасів матеріально-технічних засобів, забезпечення ними частин і підрозділів, обліку, збереження та підтримання їх у стані, який забезпечує своєчасне приведення їх у готовність до використання завдань за призначенням.

Значний вклад у розвиток механізмів державного управління логістичним забезпеченням спільних дій сил безпеки при реагуванні на кризові ситуації здійснив Бондаренко О.Г. В дослідженні *(Бондаренко О.Г., 2019)* ним розкрито теоретико-методологічні засади державного управління логістичним забезпеченням спільних дій сил безпеки при реагуванні на кризові ситуації, а саме розроблено концепцію управління логістичним забезпеченням спільних дій сил безпеки при реагуванні на кризові ситуації, що загрожують державній безпеці, обґрунтовано методичні підходи до оцінювання діяльності органів управління логістичним забезпеченням спільних дій сил безпеки на основі методів воєнно-економічного аналізу, удосконалено систему державного управління спільними діями сил безпеки при реагуванні на кризові ситуації за рахунок впровадження структурного та організаційного механізмів управління, а також організацію системи управління логістичним забезпеченням спільних дій сил безпеки при реагуванні на кризові ситуації шляхом розроблення пропозицій до нормативно-правової бази у вказаній сфері та ін.

Автором *(Бондаренко О.Г., 2019)* встановлено, що державно-приватне партнерство в сфері логістичного забезпечення наразі знаходиться в стадії становлення, а цей напрям наукових досліджень має значні перспективи. Також, ця думка підтверджується у монографічному дослідженні Бєлая С.В. *(Бєлай С.В., 2015).*

Отже, державно-приватним партнерством у сфері логістичного забезпечення сил безпеки сектору безпеки та оборони України є співробітництво між державним та приватним партнерами, що здійснюється у сфері логістичного забезпечення сил безпеки на основі та відповідно до умов договору, укладеного в рамках здійснення державно-приватного партнерства у порядку, встановленому чинним законодавством, або у будь-якій іншій формі, яка відповідає ознакам державно-приватного партнерства, визначеним законодавством України.

Головними актуальним напрямами розвитку державно-приватного партнерства у логістичному забезпеченні сил безпеки України можливо вважати наступні: виробництво (модернізація) та утилізація (демілітаризації) озброєння, військової та спеціальної техніки; будівництво (експлуатація) доріг, злітно-посадкових смуг на аеродромах, мостів, шляхових естакад, тунелів; виробництво та впровадження енергозберігаючих технологій, будівництво та капітальний ремонт житлових будинків; встановлення модульних будинків та будівництво тимчасового житла; виробництво, транспортування і постачання тепла у частини та підрозділи сил безпеки, розподілення та постачання електричної енергії; співпраця у сфері продовольчого забезпечення (аутсорсинг), а також збір, очищення та розподілення води; охорона здоров'я, надання послуг у сфері охорони здоров'я; надання освітніх послуг у сфері логістичного забезпечення сил безпеки та ін.

Додамо, що під час реалізації державно-приватного партнерства у зазначених сферах логістичного забезпечення сил безпеки вкрай важливим є організація аналізу ефективності здійснення цієї діяльності. Пропонуємо зазначений аналіз здійснювати на основі наступних заходів: детального обґрунтування економічних та екологічних наслідків реалізації державно-приватного партнерства у сфері логістичного забезпечення сил безпеки за результатами аналізу економічних та фінансових показників фінансової моделі реалізації державно-приватного партнерства, а також екологічних наслідків реалізації державно-приватного партнерства з урахуванням можливого негативного впливу на стан довкілля; обґрунтування вищої ефективності проєкту у сфері логістичного забезпечення сил безпеки із залученням приватного партнера порівняно з реалізацією проекту без такого залучення в мирний час, в умовах виникнення кризових ситуацій, а також дії особливого періоду; виявлення видів ризиків здійснення державно-приватного партнерства у сфері логістичного забезпечення сил

безпеки, їх оцінки та визначення форми управління ризиками в мирний час, в умовах виникнення кризових ситуацій, а також дії особливого періоду; визначення форми здійснення державно-приватного партнерства у сфері логістичного забезпечення сил безпеки в мирний час, в умовах виникнення кризових ситуацій, а також дії особливого періоду.

Висновки. На основі зазначеного можливо дійти наступного.

1. Становлення державно-приватного партнерства у складових сектора безпеки України сьогодні знаходиться на етапі започаткування. Наявність різних форм договірних відносин у рамках державно-приватного партнерства регулюються окремими законами та підзаконними актами, що ускладнює формування єдиного підходу до розроблення механізмів впровадження та розвитку державно-приватного партнерства.

2. Основними проблемами державно-приватного партнерства в сфері забезпечення функціонування сил сектору безпеки сектору безпеки і оборони України є: дефіцит бюджетних коштів та занадто ускладненість реалізації механізмів державної підтримки; відсутність щорічного фінансування довгострокових проєктів державно-приватного партнерства в сфері функціонування сил безпеки; невизначеність методології надання державної підтримки в рамках реалізації проєктів державно-приватного партнерства для сил безпеки; невідповідність принципів і підходів у сфері державно-приватного партнерства існуючим загальноприйнятим міжнародним принципам.

3. Для ефективного забезпечення функціонування сил сектору безпеки, крім удосконалення вітчизняної нормативно-правової бази у сфері державно-приватного партнерства, необхідне застосування механізмів управління державно-приватним партнерством у логістичному забезпеченні сил безпеки України з метою залучення приватних інвестицій на засадах такого партнерства.

4. Досліджені теоретичні засади термінів «логістика» та «логістичного забезпечення» зазначили, що найважливіше значення при розробці і створенні логістичних систем мають принципи, які визначають характер і суть усього устрою узгодження загалом і окремих його аспектів зокрема. Не менш важливе значення мають принципи логістичного забезпечення сил безпеки, що узгоджуються з законодавчими актами з питань національної безпеки та оборони України і зі стандартами логістичного забезпечення сил безпеки ЄС та НАТО.

5. Сьогодні встановлені чіткі норми та правила організації державно-приватного партнерства в Україні. Однак визначений перелік сфер реалізації державно-приватного партнерства є занадто вузьким. Зрозуміло, що законодавець залишає право державному партнеру застосовувати державно-приватне партнерство в інших сферах діяльності, які передбачають надання суспільно значущих послуг, крім видів господарської діяльності, які

відповідно до законодавства дозволяються здійснювати виключно державним підприємствам, установам та організаціям.

6. Процес прийняття рішення щодо застосування механізмів державно-приватного партнерства в сфері безпеки держави є занадто складний та не позбавлений корупційної складової. Наразі державно-приватне партнерство розвинене в основному у державному (муніципальному) секторі, а саме в житлово-комунальному господарстві, транспорті та медицині. При цьому поза увагою залишаються питання розвитку державно-приватного партнерства у сфері забезпечення державної безпеки взагалі, а у логістичному забезпеченні сил безпеки України зокрема.

References:

Бєлай С. В. (2015). Державні механізми протидії кризовим явищам соціально-економічного характеру: теорія, методологія, практика : монографія. Харків: Вид-во НА НГУ, 2015. 349 с.
Ларіна Р.Р. (2005). Формування та забезпечення надійності регіональних логістичних систем. Монографія. Донецьк: Норд-Пресс, 2005. 284 с.
Milliband, R. (1974). The State in Capitalist Society. New York.1973. Nozik, R. Anarchy, State and Utopia. New York.
Barnekov T., Boyle R. and Rich D. (1989). Privatism and Urban Policy in Britain and the United States. Oxford.
JP 4-02 – HEALTH SERVICE SUPPORT July 2012, INCORPORATING CHANGE October 2012.
Бондаренко О. Г. (2019). Державне управління логістичним забезпеченням спільних дій сил безпеки при реагуванні на кризові ситуації: дис.д-ра наук держ. упр.: 25.00.05/Національний університет цивільного захисту України. Харків, 2019. 470 с.

DOI 10.5281/zenodo.10821945
UDC 338.488.2:640.43-049.5

CHAPTER 12.
FORMATION AND ENSURING SECURITY IN THE RESTAURANT BUSINESS

Valentyna POSTOVA
PhD in Economics, Associate Professor of the Department
of Tourism and Hotel and Restaurant Business,
Vinnytsia Institute of Trade and Economics
of State University of Trade and Economics
(Soborna, 87, 21000, Vinnytsia, Ukraine)
v.postova@vtei.edu.ua
https://orcid.org/0000-0002-0056-5648

Abstract. The study examines the issues of forming and ensuring security in the restaurant business. Emphasis is placed on the importance of a safe environment for both staff and guests of the facility. Safety is one of several factors of successful restaurant business. It includes protection of staff and guests from various risks, such as: food poisoning, fires, thefts, injuries, terrorist acts. Unresolved issues are: lack of understanding of the importance of security by restaurant owners and staff, lack of a clear security system in many establishments, imperfection of the legal framework in the area of restaurant business security, lack of qualified security specialists, low level of security culture in society. In the work, a set of measures aimed at forming and ensuring safety in the restaurant business was developed. Implementation of a comprehensive security system will significantly reduce risks to people's lives and health, as well as minimize risks for the restaurant business. The level of formation and security in the restaurant business in Ukraine is insufficient. It is necessary to take measures to improve the situation, such as: development and implementation of regular security systems in restaurants, conducting training of staff on security rules, strengthening control and auditing of security systems, increasing the responsibility of restaurant owners and personnel managers for security. The results of the research can be used for: development and implementation of safety standards in the restaurant business, training of restaurant staff in safety rules, level of safety culture in society.

Keywords*:* security, restaurant business, staff, guests, risks, security system, security rules, emergency situations, control.

Introduction. Security at restaurant business enterprises is a set of measures aimed at protecting people, property and information from possible threats. This topic is extremely relevant, because restaurants and cafes are visited by thousands of people every day, and the risks of emergency situations or crimes always exist.

Ensuring security at restaurant business enterprises is determined by a number of factors: an increase in the level of crime: theft, fraud, vandalism are just some of the risks that restaurants may face; terrorist threat: terrorist attacks can have dire consequences for both people and businesses; emergency situations: fires, floods, earthquakes - such events can lead to significant material losses and human casualties; fierce competition: in the competitive environment of the restaurant business, any incident can negatively affect the reputation and image of the establishment; growing demands from the state: the authorities pay more and more attention to safety issues at restaurant business enterprises.

Ensuring security at restaurant business enterprises is an important task that requires a comprehensive approach. The recommendations developed in the course of the research can be used to increase the level of safety at restaurant business enterprises, which, in turn, will contribute to improving the quality of service and increasing the competitiveness of establishments.

During recreation, people think the least about their safety, which sometimes leads to undesirable consequences related to the risk to their lives. Therefore, the task of the administration of restaurant business enterprises is to prevent all possible risks for the life and health of their guests.

The concept of security includes not only protection from criminal situations, but also to a greater extent the creation of precautionary measures to ensure protection against fire, explosion and other emergency events, as well as in the current situation the application of measures to prevent the spread of the Covid-19 pandemic.

The main principle of using restaurant security systems is security, which cannot be ensured at the expense of guest comfort. That is why restaurant security systems, as a rule, are significantly different from «ordinary» ones, which are used in office premises and other enterprises. Therefore, the security system in restaurant establishments includes many components, which include people (security service), door locks in halls and other premises, and safes that can be used by guests of the establishment. Today, a popular and necessary event is the installation of a video surveillance system, although it sometimes causes the disapproval of guests of the establishment.

The concept of safety at restaurant business enterprises in a general sense is an officially accepted system of views on certain goals, tasks, as well as basic principles and directions in the field of ensuring the safety and sustainable development of any restaurant establishment, the life and health of the staff and guests of the establishment, their rights and freedoms – in conditions of possible

external and internal dangers and threats. The development of measures to ensure security at the enterprises of the restaurant business, the mechanism of their implementation, is carried out taking into account the threats that can oppose this object of research as a whole.

1. The essence and features of the security system in restaurants.

The following groups of threats are typical for any restaurant business enterprise: natural, man-made, ecological, terrorist and social. The danger levels of threats of various kinds may depend on the political situation in the country and in the world in general, the stability of the socio-economic development of both the country and the region as a whole.

The multifaceted nature of ensuring the safety of guests and restaurant staff, as well as tasks in the field of information protection, require the creation of a special service that can implement the necessary set of protective measures *(Balatska N.Yu., 2020)*. When organizing the security system of restaurant business enterprises, it is necessary to clearly know for what purposes and at the expense of which funds it will function. When solving security issues, restaurant managers tend to resort to two extremes: either they spend significant money on the organization of extremely complex security systems that are intended for high-security facilities, or they do not pay due attention to security issues at all.

In modern conditions, the safety of restaurant business enterprises, its employees and visitors, becomes one of the factors of increasing the competitiveness of this business. However, one should not forget that any restaurant establishment, as a commercial enterprise, is the subject of special interest of competitors in this field of business. The presence on the market of a developed system for extracting commercial information determines the legality of creating an equally developed system for its protection against unauthorized acquisition and malicious use (*Belyaeva S. S., Byshovets L. G., D Kurakin O. B., 2020*). These functions should be performed by the security services of any restaurant business enterprise. The classification of threats, including the dangers that arise during various types of interaction, indicate that in modern conditions, in order to ensure the safety of both the staff and visitors of the restaurant, as well as the restaurant itself as a commercial enterprise, separate measures and actions are necessary will not succeed That is why a constantly operating system is needed, which can cover all the variety of forms and methods of ensuring the safety of this staff, guests of the establishment and the commercial activity of the restaurant enterprise itself (*Rusavska V. A., Chebotaeva T. S., 2021*).

To create the security system described above, it is important to classify various types of dangers and threats that arise in the process of interaction between the parties. Participants of the interaction engage in both direct physical contact and informational and financial interaction, so all

threats can be conditionally divided into three categories, such as: physical, informational and financial.

Physical threats are the result of physical actions. They cause damage to people's health, their property, as well as property of the restaurant business; indirectly affect the size of profits, as well as losses.

Financial threats – cause damages, as well as direct financial losses both to the restaurant business itself and to the guests of the establishment.

Information threats are a consequence of interaction in the field of communication, which lead to indirect financial losses, as well as moral costs (*Bocharova O.V., 2019*).

One of the urgent issues of the security of hospitality establishments is the information security of the establishment, since any purposeful and unfriendly action against the interests of the enterprise begins with the collection of information. In connection with the deterioration of such components of information resources as confidentiality, integrity, availability and reliability, malfunctions in the functioning of management systems are observed, information constituting a commercial secret is disclosed, and the reliability of financial documentation is violated.

The main information threats are presented in fig. 1.

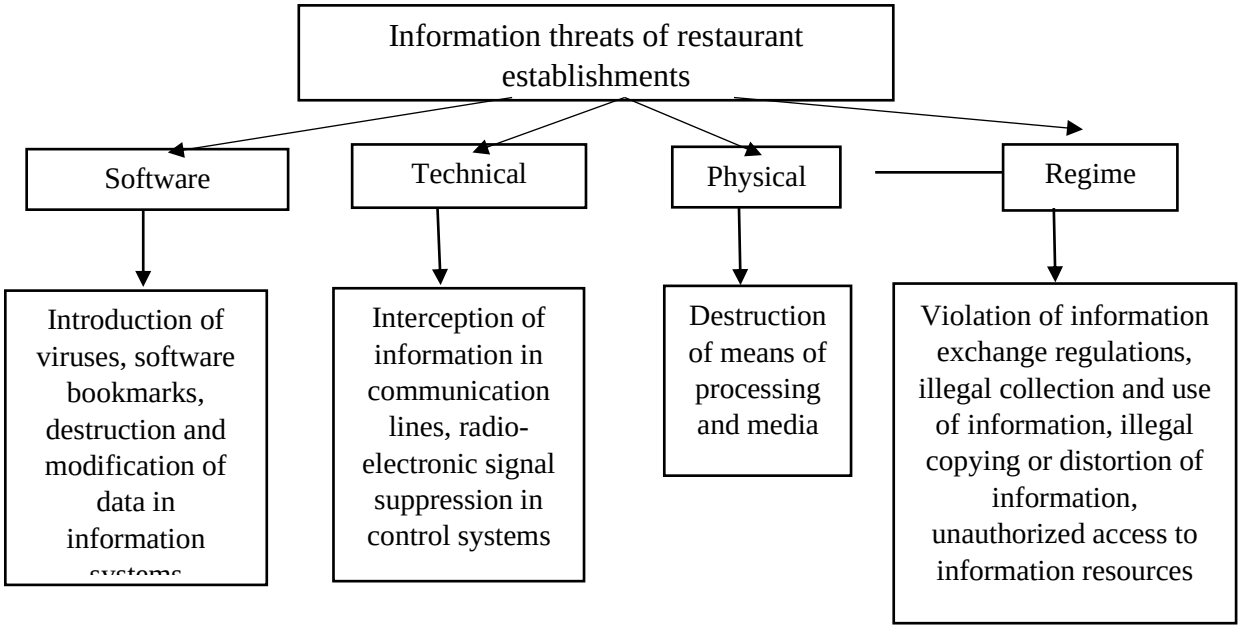


Figure 1 – Main groups of information threats in the field of restaurant industry

Analyzing information security in the field of restaurant industry, special attention should be paid to cybercrime. This is a violation of other people's rights and interests in automated data processing systems.

To ensure information security in the restaurant business, it is necessary to:

1) analyze and summarize potential threats and causes of violations;

2) develop information risk assessment methods;

3) carry out information surveys of the company's resources;

4) develop policies and concepts of information security;

5) develop a corporate standard for ensuring information security;

6) classify part of the information as restricted access (official secret);

7) monitor the operation of technical information protection measures.

Thus, in order to increase the level of security in the restaurant industry, it is necessary first of all to conduct an audit and control the functioning of the information security system in a timely manner and to have the opportunity to eliminate risks; to develop a mechanism for managing the security of the enterprise on the basis of controlling, as well as to analyze the threats of the internal and external environment.

There are various types of risk classification. Each of them allows identifying certain properties in risks. N.M. Vnukova considers the classification of risks by external and internal factors to be the most relevant for the restaurant industry (Fig. 2).

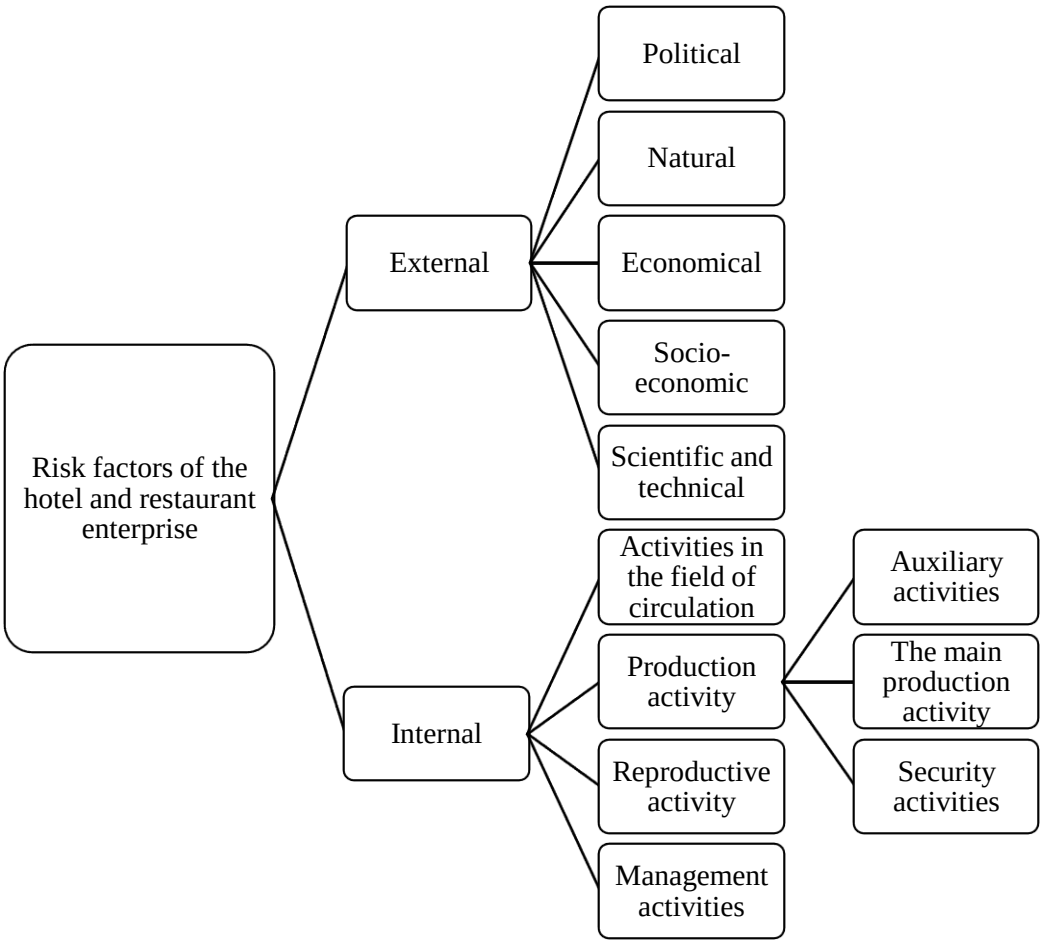


Figure 2 – Classification groups of risk factors in the field of restaurant business

In addition to the specified classification, risks in the activity of restaurant establishments can be divided into:

1. Risks, the consequences of which affect people. This group is divided into two subgroups: risks affecting staff and risks affecting visitors. These are, for example, equipment breakdowns, disasters, inadequate actions of personnel, crime and others.

2. Risks, the consequences of which affect production systems and threaten their integrity. These are, for example, disasters, thefts, equipment failure, etc.

When considering different categories of risks characteristic of the restaurant industry, it is worth mentioning force majeure or force majeure circumstances, as they differ from other types of risks in having more serious and global consequences.

In recent years, terrorism has become a serious international problem. It poses a particular danger for large establishments of the restaurant business. Terrorist attacks are becoming increasingly large-scale, multifaceted in terms of the pursued goals and types of manifestation.

Enterprises of the restaurant business, in accordance with the Law of Ukraine «On Tourism», are responsible for: preserving the belongings of customers, and are also responsible for damage caused to the life, health and property of vacationers as a result of shortcomings in the provision of services, and also compensates moral damage caused to the customer by the violation his rights (*Bocharova O.V., 2019*).

Therefore, every restaurant business enterprise must have a plan of measures to ensure the protection and safety of visitors to the establishment, which includes such risk factors as: fire, theft, injury, unexpected illness, and others. In the building of the restaurant business, all emergency exits and evacuation routes for guests of the establishment must be clearly marked, and in each hall and in all places where visitors gather, there must be visual information about emergency exits, evacuation routes, as well as the nearest fire alarm system.

The protection of guests and their property is an important aspect of the restaurant business. The owner and employees of the establishment are required by law to take all necessary precautions to ensure the safety of visitors to the establishment (including economic). Electronic management systems play a major role in this matter at the current stage of restaurant business development. They use a computer network of the latest generation, as well as the latest technologies, which help to increase the efficiency of operations and minimize annual manipulations when making calculations in the institution.

Enterprises of the restaurant business are obliged to provide their guests with information about fire safety rules, and also, if necessary, call an ambulance for visitors without additional payment (*Rusavska V. A., Chebotaeva T. S., 2021*).

But restaurants have their own safety problems. In institutions of this field of activity, all responsibilities for the control of security systems are entrusted, as a rule, to the general director *(Balatska N.Yu., 2020)*.

The area that is of particular interest to the security service in the restaurant industry primarily includes:

- storage and movement of products in the institution;
- storage and consumption of liquor and vodka products (bar products);
- settlements with guests of the establishment;
- document flow at the restaurant business enterprise.

It is very important to control the storage and movement of products in the restaurant business. Since the storage of products and the acceptance of supplies of raw materials according to the establishment's menu can be carried out without the participation of outsiders, most managers of establishments pay attention primarily to ensuring the integrity of products by their own employees and suppliers, as well as the freshness of these raw materials. Food products are a great excuse for would-be thieves.

Not only food products attract the attention of thieves, but also tableware and cooking equipment are no less attractive.

Control over liquor and vodka products, namely bar products, is also very important. Nothing needs the attention of managers interested in the integrity of the establishment's property more than the control of liquor and vodka products, because alcoholic beverages are an extremely profitable product (because they have the highest markup) and are very difficult to control. Theft of alcoholic beverages can take any form: removal from the warehouse, consumption by employees at the workplace, and concealment of profits (*Ivanyuk A., Chikunova-Vasilyeva N., 2019*).

New methods of controlling the storage and sale of alcoholic beverages made it possible to reduce losses from theft in restaurants. One of these methods is the use of an automatic dispenser directly connected to the cash register at the bar of the establishment.

Equally important is control over settlements with visitors to the institution. Service receipts are traditionally the means by which service personnel, namely waiters and bartenders, transfer guests' orders to the establishment's production facilities. In addition, invoices are payment documents that confirm the guest's indebtedness to the restaurant establishment that serves him.

There is only one way to significantly reduce the number of problems associated with the integrity of the logistics and with the billing of the dishes on the menu - is to accurately record everything that happened. After a certain time, you can clearly understand what is happening and immediately take action to prevent these problems. These records should include:

- the essence of what happened during the operation of the institution;

- date and time of the event;

- list of participants from visitors and statements of witnesses, if any;

- damage to the institution's property, if there were any;

- measures taken by the restaurant administration, including notification of local law enforcement agencies, if necessary;

- signature of the compiler of the report, as well as the date.

Quality is important, because if we consider the restaurant industry from the perspective of the dynamics of their development, then quality will have the greatest impact on their activity and competitiveness. Without a high-quality product, the institution cannot achieve its main goal, since quality is more important than profitability (*Rusavska V. A., Chebotaeva T. S., 2021*).

Control over compliance with service standards is a management area: keeping documentation, providing an assessment of the level of service achieved, measures aimed at its improvement, including additional training of personnel, improvement of discipline and creation of a strong work force of the institution.

Collective work in the restaurant industry is rarely analyzed and qualitatively evaluated, since the main reasons for this are (*Ivanyuk A., Chikunova-Vasilyeva N., 2019*):

- insufficient attention paid to the above issue;

- lack of clearly formulated management goals, as well as work standards, on which the institution's documentation should be based;

- assessment, adjustment, as well as restoration of labor activity in a restaurant business establishment;

- correct distribution of responsibilities, as well as reliable accounting methods in the researched institution.

Managers of restaurant establishments do not always want to solve problems related to complications, as well as complaints about consumer service, as well as prices that correspond to the level of this service. Claims and complaints of visitors to the institution are considered as situations in which the search for the culprit is considered more important than finding out the causes and consequences of the situation (*Moisiienko A. V., 2019*).

The prevention of the emergence of claims to the establishment of the restaurant economy should be based on reaching an agreement between the head of the establishment, the employee, and also the consumer, in accordance with the results of the employee's work, that is, the final product. This is best achieved by establishing clear standards that can be effectively monitored and enforced. In addition, the use of the concept of collective work, in particular, in «quality chains», creates the

possibility of interconnection, which is necessary to identify and eliminate the causes of complaints from the guests of this institution. However, even here there are obstacles, the main one of which may be hidden in cultural traditions, which include the right to be protected against the appearance of claims that motivate managers. But even here, problems can be solved by finding solutions and reaching a compromise.

The security system in the restaurant business has its own features that distinguish it from the security systems of other facilities. These features include:

1. Large number of people: restaurants and cafes are visited by thousands of people every day, which creates the risk of emergency situations related to panic, crowding or other factors.

2. Specifics of the work: the work of the restaurant involves the use of flammable materials, combustible substances, as well as the operation of technological equipment, which increases the risk of fire or accident.

3. Assets: Restaurants and cafes often have significant assets such as equipment, food, alcohol, cash, making them a target for theft.

4. Competitive environment: Any incident related to security can negatively affect the reputation and image of the establishment, which can lead to loss of customers and competitive advantage.

5. Requirements from the state: the authorities pay more and more attention to safety issues at public catering enterprises, which requires restaurants and cafes to comply with strict rules and regulations.

Taking into account these features, the security system in the restaurant business should include the following components:

1. Fire safety: fire alarm system, automatic fire extinguishing system, fire extinguishers, evacuation exits, evacuation plans.

2. Security: video surveillance system, security alarm system, physical security.

3. Technological security: access control system, product accounting system, technological equipment monitoring system.

4. Information security: information protection system, data backup system.

5. Personnel: training personnel in safety rules, conducting briefings, practicing actions in emergency situations.

It is important to note that the security system must be comprehensive and take into account all possible risks and threats.

In addition, the security system must be constantly updated and improved to meet modern challenges.

Ensuring security in restaurant business establishments is the key to successful business, preservation of life and health of people, as well as protection of property and information.

2. Types of security systems in restaurant complexes: nuances of management.

It has already happened that restaurants are an industry where the traditions of theft are historically strong. Theft methods are "polished" and passed down from generation to generation. Moreover, these methods are so sophisticated that it becomes a shame that unusual intellectual potential is used for such obscene purposes. But it is necessary to fight against theft, and it is necessary to do it professionally. In fact, this is a simple task that simply needs to be solved using a systematic approach and a set of certain tools.

Types of security systems of restaurant establishments are presented in fig. 3.

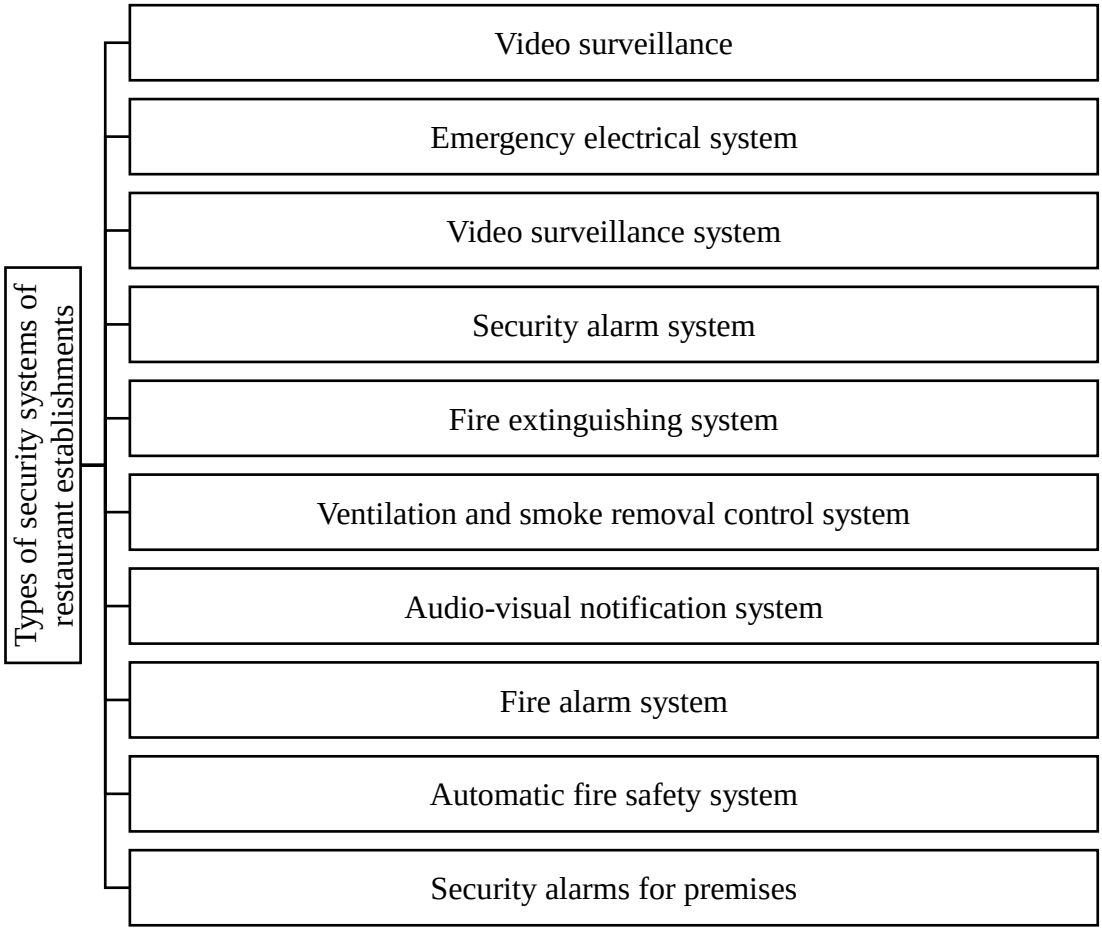


Figure 3 – Types of security systems of restaurant establishments

Technical design systems ensure the safety of restaurant establishments in emergency situations, they include: autonomous design systems (fire extinguishing, sound warning, access control systems), integrated design systems (security and fire alarms) and a comprehensive computer system for the establishment's automation.

The types of security systems of restaurant establishments include:

- means of video surveillance;

- security alarm system for premises of institutions;

- security alarm system for the perimeters of the facility;

- fire alarm in the room;

- fire extinguishing systems in the restaurant industry;

- gate automation (barrier or automatically retractable gate);

- video and audio intercoms at the entrance to the territory of the institution;

- equipment for restricting access to premises, audio monitoring of premises and telephone lines (*Omelchuk S.S., 2019*).

Video surveillance is the main control tool. The installation of this video surveillance system and the access control and management system are today mandatory, and sometimes the main element of any modern security system in restaurant establishments.

The main tasks of security video surveillance at enterprises of the restaurant business are the following:

- ensuring the safety of a large number of people visiting restaurants;

- ensuring the preservation of property of the restaurant business enterprise;

- control over the safety of personal belongings and money of visitors to the institution;

- control over the actions of the institution's service personnel;

- ensuring the absence of theft among personnel.

The video surveillance system at the enterprises of the restaurant business allows you to control the work of the staff. Thus, with the help of video surveillance in these institutions, the management can accurately monitor the amount of tips and ensure that the service staff does not deceive the visitors of the institution and does not commit fraud. The image of the restaurant industry depends on the level of service provided to guests of the establishment and the absence of fraud (*Danylenko-Kulchytska V. A., 2022*).

Thus, modern video surveillance in restaurant establishments can provide detailed monitoring of the quality of service to visitors of the establishment. Video cameras with high image quality provide a continuous, detailed recording of what is happening.

The purpose of implementing a video surveillance system at restaurant business enterprises is primarily to control the quality of service to visitors of the establishment, as well as the work of the staff, their safety, the ability to observe the area of preparation of orders, as well as the storage premises of the catering establishment.

The main components for the organization of television surveillance are television cameras (both black and white and color cameras are currently used in video surveillance), lenses, monitors, squarers, multiplexers (process signals from video cameras), special video recorders. In addition,

various brackets, rotary devices, casings, amplifiers, modulators are used. The specific composition of the equipment depends on the number of cameras, the conditions of their operation (outside the facility or inside the premises), distances between cameras, as well as monitors (observation post) (*Rusavska V. A., Chebotaeva T. S., 2021*).

It is recommended to install video cameras in restaurant establishments in places where control is especially necessary:

1) in the shopping hall for guests of the establishment - this is an area subject to mandatory video surveillance. The location of the video cameras is determined based on the specifics of the layout of this trading hall. Video monitoring is important from the point of view of the quality of service to the visitors of the institution and their safety, as well as the ability to objectively evaluate the work of the staff;

2) one of the important purposes of the video surveillance system in the checkout area (bar counter) is not only the prevention of theft, but also the detection of fraudsters, which is greatly helped by working with the video archive.

One of the components of the security system is the access control and management system (ACMS). The principle of operation of this system is as follows: each employee of a restaurant establishment receives an electronic key - a plastic card or a biometric reader (fingerprint reader) with the content of an individual code in which the data of the owner of such a card is entered: photo, video images, structural subdivision of the restaurant establishment business and other information about the owner, with the help of which the passage of employees through turnstiles or barriers is organized.

The system of control and management of access to establishments of the restaurant business allows you to conduct:

- accounting of working hours of employees of the institution;
- carry out identification of an employee of the institution;
- exercise control over the movement of employees - going out for smoke or coffee breaks;
- provide protection against transferring the card to another person;
- allows to solve issues of safety and discipline at the workplace;
- automate personnel and accounting records in the institution;
- to create an automated workplace of a restaurant business guard.

Security alarms for restaurant premises can be divided into stationary and mobile. A simple example of a stationary device is an alarm button, when pressed, information about an attack on a given enterprise is transmitted to the security of the establishment (*Danylenko-Kulchytska V. A., 2022*).

The purpose of the perimeter security alarm system is to detect the trespasser as early as possible, even before he enters the guarded restaurant establishment, in order to prevent any undesirable consequences. That is why such security systems are the most effective means of protection against unauthorized entry, because they give an alarm signal long before an intruder can penetrate into particularly important areas of restaurant business enterprises.

Also, in terms of safety, the fire alarm system (SPS) of an "intelligent" restaurant business enterprise is very important, which is built in such a way that the automatic control systems for life support, fire alarm, as well as control of the automatic fire extinguishing system are performed in a single information space. Direct and unconditional interaction is organized between these systems. SPS integrates with other systems of the security complex of the restaurant industry.

Fire alarm systems that support tens of thousands of address-analog annunciators, as well as loops, are used to protect restaurant business enterprises that occupy a large area.

The SPS of the «intelligent» enterprise of the restaurant business is maximally «open» for programming and configuration, which allows it to be perfectly adapted to the characteristics of the premises of these protected establishments. This system has a high degree of reliability: an alarm signal is generated only after multiple confirmations from the annunciator, so that false alarms are practically excluded, and sensitivity levels and trigger thresholds can be set depending on the time of day and day of the week, and pre-trigger levels are automatically set, which increases the probability of detecting an outbreak at an early stage. In addition, the SPS allows preventive fire-fighting measures to be carried out in areas located in the immediate vicinity of the outbreak site on the territory of restaurant establishments. Fire extinguishing devices and systems used in restaurant business establishments: the purpose of these systems is to automatically extinguish fires and prevent the spread of fire.

The following system construction options are possible:

1. According to the principle of fire extinguishing:

- sprinkler fire extinguishing (the cheapest option under the condition of complete reconstruction of the restaurant business enterprise);

- aerosol or powder fire extinguishing;

- gas fire extinguishing (high efficiency, does not harm the interior of the restaurant).

2. According to the principle of system organization:

- autonomous modules with built-in fire sensors;

- the command to turn on this module will be given by the central fire station or integrated security system.

The purpose of the ventilation and smoke removal system is necessary to prevent the spread of smoke, as well as fire through elevator and ventilation shafts and pipes, smoke removal from the premises of the restaurant business.

This system consists of the following subsystems:

- smoke removal (the central fire alarm station generates signals that start the corresponding electric motors of the ventilation system);

- preventing the spread of smoke (the central fire alarm station generates signals that control the shutter drives of the ventilation system, starts the electric motors of the turbines, which create increased pressure in the elevator shafts) (*Yermoshenko M.M., Horyacheva K.S., 2019*).

Access control systems are also used in restaurant establishments, which help to ensure not only the preservation of material values and information, but also the safety of staff and visitors of this establishment. At a modern level, they solve the tasks of ensuring safety, improving labor discipline, as well as automating personnel and accounting records in various departments of the restaurant business. In addition, the installation of this system of limited access to the premises will significantly increase the efficiency of the security service of the restaurant business enterprise (*Honcharenko N. V., 2021*).

Thus, the application of the described security measures will not only protect visitors of the establishment during their stay at the restaurant business enterprise, but also protect employees from unfounded accusations. And this, along with other aspects, will increase the institution's reputation and, as a result, increase its rating.

Every restaurant business has the goal of making a profit. But this can be hindered by fines from the regulatory authorities. Therefore, occupational health and safety in restaurants is the first step for successful business (*Kupchak B.F., 2019*).

Restaurant establishments can vary in size – from small, cozy coffee shops to large restaurant complexes, and each such establishment has several functional departments: production premises where, in fact, meals are prepared, a service for providing goods and a sales hall for visitors.

The restaurant establishment is served by a whole staff of staff - cooks, waiters, bartenders, administrators. Occupational health and safety in these establishments is very important in the process of organizing a restaurant business, because very often the work exposes workers to serious dangers associated with the use of sharp and heavy objects, special machines, freezers, equipment for processing products with steam and cutting (*Honcharenko N. V., 2021*).

Getting injured while working is, unfortunately, a common thing. That is why it is quite necessary to prevent similar situations in order to avoid fines, court proceedings, and stress.

Occupational health and safety in restaurants is a comprehensive solution that will help avoid problems related to the safety of this business. Conducting an assessment of the state of labor protection at the enterprises of the restaurant business will help to identify shortcomings in the labor protection system. This will contribute to the formation of a safe production environment, as well as reducing the level of industrial injuries, occupational diseases of production and service workers, dangerous accidents and the overall success of the restaurant business (*Ivanchenko N.O., 2019*).

Experienced occupational health and safety specialists will offer standardized work processes where the employee clearly knows their responsibilities, provide appropriate training to the facility's personnel, and help to establish constant control over compliance with occupational health and safety rules.

In order for a restaurant business to be successful, it is very important to be able to constantly receive qualified advice on any issues related to occupational health and safety. Experts in this field will help to quickly deal with any difficult situation that could arise at restaurant business enterprises, organize the necessary training for the staff of the institution, as well as the passing of medical examinations by employees (*Yermoshenko M.M., Horyacheva K.S., 2019*).

The business success, as well as the reputation of any restaurant establishment, depends to a great extent on how successfully these establishments pass regular inspections by local health authorities. Problems with non-compliance with certain sanitary standards can be guaranteed to be avoided if the management, as well as the employees of the establishment, consider ensuring food safety as a top priority in their own activities. At restaurant business enterprises, sanitary and hygienic norms and rules established by sanitary and epidemiological supervision bodies regarding the cleanliness of premises, the condition of sanitary and technical and production equipment, waste removal, and effective protection against insects and rodents must be observed.

Therefore, the implementation of the practice of strict compliance with sanitary and hygienic standards depends on the management of the restaurant industry, because it is they who are authorized to dispose of funds for training and training of personnel, as well as for the purchase of improved and newer models of restaurant equipment.

Special requirements in relation to safety are imposed on service personnel in the institution. First, all personnel must be trained in safe work methods at the facility, know and follow fire safety, occupational health and safety regulations. All employees of a restaurant business enterprise must be subject to a periodic medical examination, and upon being hired, they are required to undergo a medical examination, as well as attend a course on sanitary and hygienic training (*Matskiv O. O., Shah A. Ye., 2014*).

Restaurant establishments that care about the safety of their visitors organize regular additional seminars for employees of production departments, namely the kitchen. The purpose of these seminars is to remind the staff of the need to follow the rules of sanitation and hygiene and thus prevent the danger of spreading infections. In the process of working at restaurant business enterprises, service personnel must periodically, at least once every 2 years, pass examinations on the sanitary minimum. A personal medical book is established for each employee of the institution, in which the results of medical examinations, records of transmitted infectious diseases, as well as the passing of the sanitary minimum are entered. Persons who spread infectious diseases are not allowed to work in restaurants.

Most often, food infections spread in restaurants due to the dirty hands of the staff, which is why it is worth monitoring the amount and frequency of hand washing by the staff of the production facilities (cooks, their assistants, waiters). Therefore, it is not enough to use ordinary soap, and you need special disinfectant soap or detergents, and you should use disposable towels to wipe your hands.

For example, fast food establishments - McDonald's, have strict rules regarding sanitation, which provide for 10 cases when service personnel must wash their hands (*Stelmashchuk N.A., 2019*):

- after smoking in a specially designated area;
- after eating (during the break);
- after visiting the toilet;
- before starting work from the beginning of the working day;
- after washing the floor, as well as changing the trash cans;
- after touching your own uniform;
- after sneezing and coughing;
- after changing the working area during the working day;
- after working with money (settlement for orders with visitors);
- after touching your own hair and face.

It is possible to introduce a number of actions that will convince the management of the need to pay financial attention to this particular problem – ensuring safe food (*Luhova V.M., 2019*):

- more often tell regional level managers «scary» stories about how non-compliance with sanitary standards resulted in large losses and fines for one of the offending restaurant establishments;
- to convince family-oriented managers that the introduction of safe technologies will make it possible to more reliably protect visitors of the institution, who come to this institution with children and relatives, from trouble;
- invite managers of restaurant establishments to meetings of employees where ServSafe classes are held, so that they listen to, look at slides, as well as graphic materials.

Being impressed, they will listen more carefully to the information that disadvantaged areas of the restaurant industry need additional funding for training and improving operations:

- ServSafe certificates obtained by the management can be hung on the walls in the lobby of the restaurant;

- distribute press releases emphasizing that the success of inspections depends on how well and fully the management supports the idea of certifying all employees according to the selected ServSafe program.

3. Priority directions for restaurant security.

Restaurant establishments, which are experiencing a period of self-isolation and have returned to serving visitors in the hall, had to adapt to a completely new reality and look for new tools in the competition for visitors. Visitors returned only to those establishments where they felt more protected. This applies not only to the entire supply chain of products, but also to architectural solutions.

Therefore, restaurants will have to review the planning and approaches to the zoning of halls. Dense seating will be a thing of the past. The intervals between tables will increase - or large spaces will be divided into smaller sections. Before this pandemic, the norm in European restaurants was about 1.4 square meters. m for one seat.

The World Health Organization (WHO) recommended increasing it to 2.5 square meters. m per visitor. However, more than a quarter of respondents think that the distances between tables in restaurants will return to the old norms already at the end of this year, but certain measures of social distancing will remain until the end of 2021 (*Polotai B.Ya., Zhmur-Klymenko B.V., 2022*).

Another trend in the organization of space that can be used in restaurants is an open kitchen, when the process of cooking can be observed through the glass, so that there is no doubt about compliance with sanitary standards. All reusable and previously hand-to-hand items will be replaced with disposable or easily sterilized items. All necessary sauces and seasonings in restaurants must be in individual packaging.

It is also worth abandoning paper menus in the restaurant, so dishes will be chosen on the smartphone screen via QR codes or on restaurant tablets with an antimicrobial coating of the screen.

Disinfecting napkins and sanitizer should be used as a common element of serving in a restaurant, and cutlery must be served in packaging after disinfection - like manicure tools in a beauty salon.

57% of surveyed restaurant visitors via social networks noted that they would feel more comfortable in a restaurant, they would now be helped by "regular and visible hygiene of tables, partitions and other interior elements touched by other people", more than 40% would be happy with

disinfectant wipes, serving food in closed dishes, increasing the distance between tables and the absence of common tables.

Antibacterial fabrics, as well as composite materials and self-cleaning surfaces, are often used in restaurant decoration. For example, copper and alloys with a high copper content have antibacterial and antiviral properties.

Also, restaurants should move towards greater automation and be equipped with contactless technologies: automatic doors, lighting, supply of water, soap and paper in restrooms should become mandatory elements.

Approaches that have long been accepted and mandatory in the processing of medical institutions can be transferred to objects of the restaurant business. This is, for example, a reduction in the number of surfaces on which dust or microbes accumulate, increased requirements for ventilation and air purification systems. Therefore, it is worth reviewing the interior of restaurants, reducing the number of paintings in the shopping halls of the institution, as well as reviewing the decor in the premises of this restaurant.

Also, the priority areas of ensuring the safety of the restaurant by technical means are:

- control of access to the restaurant;
- a set of measures for fire protection in the institution;
- security alarm, as well as video surveillance (*Yermoshenko M.M., Horyacheva K.S., 2019*).

The installed complex of means and protection systems in the restaurant must be adequate to the possible threat, that is, the means and systems must be self-sufficient. It is impossible and impractical to exclude the possibility of damage primarily for economic reasons.

Security devices are quite expensive, so their choice should be determined by a really smart analysis of the highest risks and losses that can occur in the restaurant.

All applied measures and means should not create any danger to the health and life of restaurant visitors and employees of the restaurant business establishment, which primarily concerns the provision of emergency action in an emergency situation.

The centralized security alarm system in the restaurant is the center of ensuring the safety of the life support zones of the recreation facility, preventing uncontrolled entry into the premises.

To ensure constant monitoring of alarm signals, the receiving and control device is located in a place where personnel are constantly present (it can be a security control room or a restaurant bar).

Therefore, the restaurant must be equipped with security alarms:

- emergency exits from the restaurant;
- external doors that are usually closed;
- doors of service premises with equipment that usually works without service personnel;

- the doors of a number of critical premises of the restaurant, the protection of which must be ensured when they are not actively used (*Parpan T. V., 2019*).

In those places where special precautions are required due to the objects located there, it is necessary to install traffic warning signs. The security alarm system in the restaurant should be equipped with sound and visual alarm devices (buzzer, siren, lanyard alarms), which should draw the attention of the staff of the restaurant under investigation to an alarm situation.

It is also necessary to provide a centralized video surveillance system in the restaurant. The system should provide the ability to observe in real time, as well as make a record of what is happening for further study.

It is necessary to ensure the recording of all video cameras in the restaurant on a VCR. The main surveillance monitors, switching equipment and recording devices should be installed in the premises of the security service or the guard on duty.

It is also worth installing additional video cameras: in the production premises (kitchen) of the restaurant, at the entrance to the establishment, near the dressing room.

Video cameras should cover areas where food is prepared, so that it is easy for restaurant management to monitor food preparation processes, as well as compliance with sanitary standards. To minimize the risks of theft and damage to products and other material assets, we recommend, in addition to video cameras, to install electromagnetic locks that can be opened using electronic keys (code, key fob, plastic card) (*Titomyr L., Vlasiuk K., 2022*).

Thus, it will be possible to restrict outsiders' access to the premises of the restaurant, where food, dishes, kitchen equipment are stored, as well as to control materially responsible persons.

We recommend installing anti-vandal video cameras with a high class of protection against external environmental influences (IP65 or IP66) near the entrances to the restaurant premises and around the perimeter, as well as a built-in infrared illumination with a range of at least 30 meters. This will allow the restaurant guard to get a high-quality image in any weather (rain, snow, high cloudiness).

To protect the restaurant business from intruders (burglars, hooligans who try to break the glass, robbers), it is worth configuring the functions of motion detection and sending alarm messages in the cameras.

Therefore, all measures and means used should not create additional danger to the health and life of visitors, as well as restaurant employees. This concerns, first of all, the provision of emergency evacuation in an emergency situation.

We can improve the food safety system in the restaurant by implementing the HACCP (Hazard Analysis Critical Control Point) system in this institution – international standards for reducing the risk of food safety.

For this, it is necessary to develop and register technical documentation for the most important (critical) processes in the restaurant.

The HACCP system in a restaurant depends on the format of the establishment, where some critical processes may differ. But there are main points that should be taken into account when developing this food safety system:

- general procedures for using equipment in the restaurant kitchen and bar;
- instructions for the restaurant staff in compliance with the relevant hygiene standards;
- cleanliness monitoring system in the restaurant premises, as well as rules for its maintenance;
- instructions for preparing all dishes from the restaurant menu;
- procedure for obtaining products from the suppliers of the researched institution;
- rules for transporting raw materials to the restaurant;
- recommendations regarding the process, as well as the temperature of food storage in this restaurant;
- instructions on the terms of preparation, as well as serving dishes to restaurant visitors.

The State Production and Consumer Service has the right to check the operation of the restaurant in accordance with the legislation on food products. The procedures for such control are determined by Law No. 2042, which entered into force on April 4, 2018.

Since September 2019, all establishments of the restaurant industry had to be inspected in a mandatory manner. In connection with the beginning of the spread of the Covid-19 coronavirus pandemic, these inspections have been postponed, which means that establishments can implement this HACCP system during this time.

To get started, restaurants must register their production facilities:

1. Submit an application to the territorial body of the State Production and Consumer Service.

2. The application must be submitted by the director of the restaurant 10 days before the opening of the establishment.

3. The territorial body makes a decision and, if everything is completed correctly, issues an order on state registration (*Honcharenko N. V., 2021*).

Based on seven principles, the HACCP system is a set of rules for the organization of production activities, which guarantees the provision of a high-quality and safe product for the consumer. Each enterprise, whose products pass the way from the state of raw materials to the

consumer, acting in accordance with the principles of HACCP, will provide people with a safe product (Fig. 4) (*Moroz O. V., Karachina N. P., Shiyan A. A., 2019*). Consider these principles:

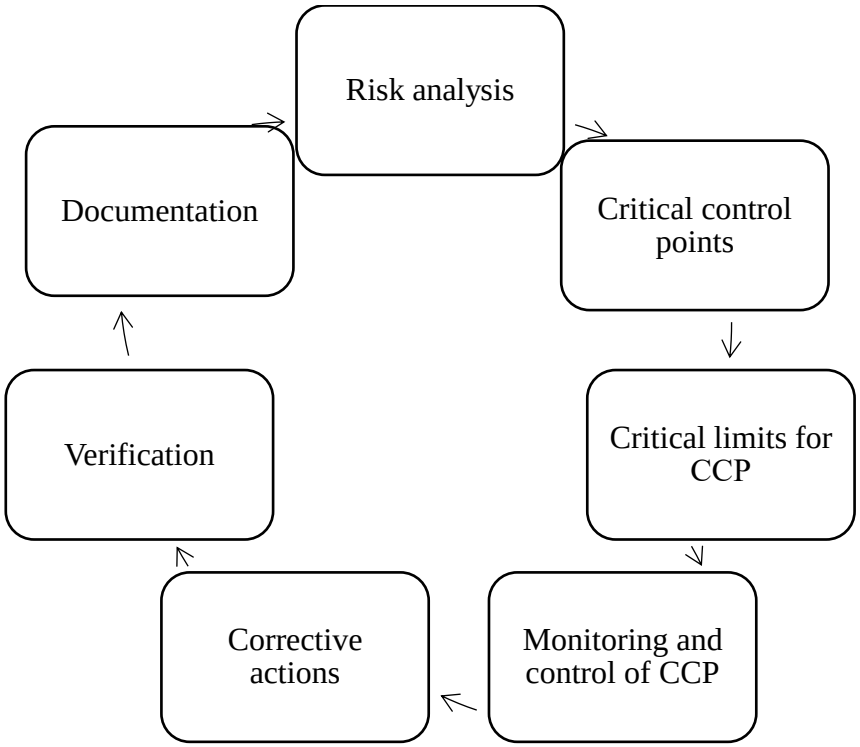


Figure 4 – Principles of the HACCP system

Principle 1. Carrying out risk analysis. The essence of the principle consists in the study of all factors related to the production of products (from raw materials to storage of the finished product in the warehouse), which can affect its safety for the consumer; compilation of lists of production operations in which these risks are possible; developing a list of precautionary measures to control these risks.

Principle 2. Determination of critical control points (CCP). In this principle, the definition of critical stages of the technological process, which affect the safety of products, is assumed. After the analysis of risks and dangers, the obtained information is used to determine specific stages of the production process, which are critical points.

Principle 3. Establishing the critical limits of each CCP. The task is aimed at establishing critical limits, upon reaching which measures should be taken to prevent the development of identified risks at one or another critical control point.

Principle 4. Establishment of a system of monitoring of CCP. After determining the critical control points and optimizing their indicators, a control procedure is developed. Such a control system includes all observations and measurements of the state of the CCP in order to comply with critical limits.

Principle 5. Establishment of corrective actions. In the developed HACCP plan, corrective actions should be clearly defined, which should be taken immediately in the event that the values of its indicators for a specific CCP exceed the established limits. This principle assumes that for the safe production of products, a clear concept of the organization of production with a quick response to the prevention of risk factors is a prerequisite.

Principle 6. Establishing a recording procedure. This principle obliges to develop an effective accounting procedure for the organization and functioning of the entire HACCP system with the maintenance of appropriate documentation.

Principle 7. Establishing procedures for checking the HACCP system. Effective compliance with the HACCP plan requires systematic audits. During the first inspection, the audit commission confirms the ability of the system to adequately and fully resist existing risks (*Postova V. V., 2022*).

The seven principles of HACCP are the basis on which HACCP is based as a product safety management system. In their essence, the principles are a task, the consistent solution of which allows for the development and implementation of mandatory procedures for the company's personnel.

The main goal of HACCP is to protect the health of consumers. This will be achieved if the possible and potential hazards of food production are eliminated.

At the end of 2021, the main problem of Ukrainian restaurateurs was the prolonged impact of COVID-19. Then, as the restaurant industry began to recover from the pandemic in 2022, Ukrainian restaurateurs again faced unprecedented challenges caused by the war with Russia (*Protsak K., Peredrii M., 2022*).

Russia's military invasion of Ukraine changed the life of our entire country. Many people have lost their jobs or are physically unable to work as before. In the first months of the war, the activity of restaurants practically stopped.

Restaurateurs during the war are faced with specific problems that affect the efficiency and success of the restaurant business.

The war created numerous problems in restaurants that require careful consideration and effective solutions. The safety of guests and staff becomes a top priority and every possible measure must be taken to ensure safety. Reduced demand and economic constraints require adaptation of marketing strategies and financial planning.

Ukrainian restaurateurs need to adapt to new business conditions. The use of foreign experience of anti-crisis management in restaurants during the war is relevant.

It is important to have an advanced wartime management plan. The main goal of the plan to improve the management of the restaurant during the war is to ensure the safety of guests and staff

and the effective functioning of the restaurant even in conditions of conflict (Table 1) (*Rusavska V. A., Chebotaeva T. S., 2021*).

Table 1 – Wartime Restaurant Management Improvement Plan

Name of the event	The essence of the event	Responsible
Threat assessment	It is worth carefully analyzing the potential threats associated with war or conflict in your region. It is also worth considering local conflicts, terrorist acts, the possibility of evacuation and other factors.	Restaurant owner and manager
Creation of an extraordinary committee	It is important to form a committee of representatives of various departments of the restaurant. This committee would be responsible for the development and implementation of the wartime management plan.	Owner, restaurant manager, chief administrator and sous chef
Access control and security	Access control systems, including physical barriers, video surveillance systems and security devices, should be reviewed and improved. It is important to follow up on the provision of everything necessary for safety. The restaurant must have backup power plants and systems fire safety.	Owner, restaurant manager, chief administrator and sous chef
Evacuation plans	Detailed evacuation plans and procedures for staff and guests must be developed. Evacuation drills and training should be conducted, including the use of emergency exits, escape routes and assembly points.	Owner, restaurant manager, chief administrator
Connection and communication	It is necessary to ensure proper communication with the outside world, including local authorities, suppliers. An instant messaging system and mobile means of communication for communication with staff and guests must be established.	Restaurant administrator
Stock supply	It is important to stockpile essential materials such as food, water, medicine and other necessary supplies.	Restaurant administrator
Training and learning	An equally important point is the conduct regular training and drills with staff on emergency situations, including safety procedures, first aid, fire safety and other important aspects.	Owner, restaurant manager, chief administrator
System of psychological support	Psychological support must be provided for staff and guests, as war can have severe emotional consequences. Information and resources for managing stress should also be provided psychological difficulties.	Owner, restaurant manager, chief administrator and sous chef
Monitoring the situation	It is important to constantly monitor the situation, receive updates on the current state of the conflict and follow the instructions of the relevant authorities and experts.	Owner, restaurant manager, chief administrator

This plan should be flexible and updated as the situation changes. It is important to have a clear plan and a team ready to act in case of war to ensure the safety and security of everyone in the restaurant.

We offer the following suggestions for improving restaurant management during wartime:

1. Develop contingency plans: It is important to create detailed contingency plans that take into account the potential risks and challenges of wartime. They should include evacuation procedures, safety measures, contact information for local authorities and other necessary actions.

2. Improving security: a security audit should be conducted and the access control, detection and monitoring systems of the premises should be improved. Consider working with local law enforcement to provide additional restaurant security.

3. Flexibility in services: it is necessary to consider the possibility of expanding the range of services and adapting them to the needs of customers during the war.

4. Crisis Communications Plan: A wartime communications plan must be developed that includes ways to contact guests, staff, and local authorities. The plan should provide a clear procedure for informing about possible changes in the mode of operation, safety and other important issues.

5. Staff training and education: It is important to ensure that staff are trained in emergency procedures, including first aid and evacuation skills. Regularly conduct training and practical scenarios to test the readiness of personnel to act in crisis situations.

6. Reservation and Management of Resources: Develop a system for reservation of resources such as electricity, water and food to ensure resilience during wartime. Monitoring and efficient use of resources can help avoid problems with insufficient supply. These suggestions can help improve restaurant management during wartime and ensure safety, efficiency, and satisfaction of customer and staff needs.

Developing a restaurant in a time of war can be a challenging task due to the unstable situation and security threats. However, even in such circumstances there may be certain prospects for development. Here are some possible ways to develop a restaurant:

1. Specialization in service. One must focus on specific market segments or customer groups that may have special needs or requirements during wartime.

2. Ensuring security and protection. It is necessary to improve security systems and offer services that will help guests feel safe. For example, this may include additional security measures, expert security advice, security, etc.

3. Strengthening marketing and public relations. Attention must be paid to marketing efforts aimed at drawing attention to the restaurant in wartime.

It is worth remembering that the development of a restaurant in the conditions of war is a difficult task, and it requires deep analysis and planning. Depending on specific circumstances, there may be other perspectives and opportunities. The main priority is always the safety of guests and staff, so be prepared to adapt to changes in the situation and take the necessary measures to protect them.

Prospects for further research are:

1. Improvement of security systems:

- development and implementation of new technologies to ensure security, such as biometric access control systems, surveillance cameras with artificial intelligence, automatic fire extinguishing systems;

- integration of security systems with other restaurant systems, for example, with the restaurant management system (POS) (*Ribun M.V., 2019*).

2. Improvement of personnel qualifications:

- development and implementation of safety training for restaurant staff;

- creation of online security courses for personnel;

- involvement of security specialists in the development and implementation of security systems in restaurants.

3. Development of new safety standards:

- development and implementation of new safety standards for restaurants that take into account the specifics of the restaurant business;

- creation of international safety standards for restaurants.

4. Study of the impact of security on the restaurant business:

- research on the impact of a safe environment on restaurant staff (productivity, motivation, loyalty);

- research on the impact of a safe environment on restaurant guests (satisfaction, loyalty, repeat visits);

- a study of the impact of a safe environment on the restaurant's financial indicators.

5. Studying the experience of other countries:

- study and implementation of best practices for ensuring safety in restaurants of other countries;

- cooperation with international organizations on safety issues in the restaurant business.

6. Use of artificial intelligence:

- development and implementation of artificial intelligence systems for forecasting and prevention of emergency situations in restaurants;

- using artificial intelligence to analyze safety data and develop recommendations for restaurants.

7. Environmental safety:

- research on the impact of the restaurant business on the environment;

- development and implementation of measures to reduce the negative impact of the restaurant business on the environment.

8. Economic security:

- research of risks for the economic security of restaurants;

- development and implementation of measures to protect the economic security of restaurants.

9. Personal safety:

- research of risks for the personal safety of restaurant staff and guests;

- development and implementation of measures to ensure the personal safety of restaurant staff and guests.

10. Cyber security:

- research of risks for cyber security of restaurants;

- development and implementation of measures to protect the cyber security of restaurants.

Further research on the topic of forming and ensuring safety in the restaurant business will allow:

1) increase the level of security in the restaurant business;

2) save people's lives and health;

3) minimize business risks;

4) increase the competitiveness of restaurants.

Conclusion. So, it was determined that at any restaurant business, first of all, the following should be ensured: the safety of the lives of visitors and employees of the establishment, the health and property of the guests of the establishment under normal conditions, as well as in extreme situations.

Studies have shown that the hospitality industry has to deal with many challenges and threats of modern society. Threats that arise as a result of technical failures, human factor or «informational intervention» are considered, forcing to rethink methodical and technological approaches to ensuring the safety of guests of restaurant establishments, staff and virtual information space of the restaurant space. A comprehensive approach to ensuring the safety of guests, staff and the commercial component of a restaurant enterprise is not always effective.

It was determined that safety is achieved through the effective operation of the restaurant's security service, the use of advanced innovative technologies for access, surveillance, fire prevention, and signaling.

In order to increase the level of security of industrial enterprises, it is necessary, first of all, to conduct audits and control the functioning of the information security system in a timely manner and

to be able to eliminate risks; to develop a mechanism for managing the security of the enterprise on the basis of control and analysis of threats from the internal and external environment.

Restaurant establishments use a variety of means to protect visitors, employees, and company property from external and internal threats. Such systems include: automatic fire systems, fire alarm systems, video surveillance and security alarm systems, ventilation and smoke removal control systems.

To improve the operation of the restaurant's security system, the key tasks are: identifying new criteria for assessing the level of ensuring the security of the restaurant's operation; improvement of existing and development of new methods of assessment of real and potential occupational safety threats of restaurant workers in the course of their specialized activities; active implementation of measures aimed at improving the existing security systems in the management of the restaurant's production and economic activities; carrying out activities aimed at constant improvement of existing and development of new methods of increasing the level of professional qualifications of security service personnel; prevention and minimization of the probability of incidents that harm the life and health of employees, guests, corporate clients of the restaurant, which will lead to a significant increase in the level of public safety in the institution, increase its attractiveness for visitors, profitability, financial and economic stability and investment attractiveness.

Reference:

Балацька Н.Ю. Ресторанний бізнес в умовах пандемії коронавірусу, проблеми та напрями трансформації моделей розвитку. *Інфраструктура ринку*. 2020. Вип. 42. С. 117–122. URL: https://doi.org/10.32843/infrastruct42-20 (дата звернення: 10.02.2024).

Бєляєва С. С., Бишовець Л. Г., Д Куракін О. Б. Нормативно-правове регулювання безпечності та якості харчових продуктів в Україні в сучасних умовах. *Економічна стратегія і перспективи розвитку сфери торгівлі та послуг*: збірник наукових праць ХДУХТ. 2020. №. 1 (31). С. 257-268.

Бочарова О.В. HACCP і системи управління безпечністю харчової продукції: Підручник. Одеса : Атлант, 2019. 376 с.

Гончаренко Н. В. Реорганізація ресторанного бізнесу в умовах пандемії коронавірусу COVID-19. *Держава та регіони.* 2021. №. 3. С. 120. DOI: https://doi.org/10.32840/1814-1161/2021-3-6

Даниленко-Кульчицька В. А. Вплив війни на готельно-ресторанний бізнес України. *Індустрія туризму і гостинності в Центральній та Східній Європі*. 2022. №. 6. С. 19-23. DOI: https://doi.org/10.32782/tourismhospcee-6-3

Єрмошенко М.М., Горячева К.С. Фінансова складова економічної безпеки: держава і підприємництво: монографія. Київ: Національна академія управління, 2019. 232 с.

Іванченко Н.О. Інформаційна складова економічної безпеки підприємства та її значення для забезпечення стійкого розвитку національної економіки. *Стратегія розвитку України*. 2019. №3. С. 124-128. URL: URL: https://jrnl.nau.edu.ua/index.php/SR/article/view/4296/0

Іванюк А., Чикунова-Васильєва Н. Забезпечення безпеки та якості харчових продуктів за чинним законодавством України. *Проблеми охорони праці, промислової та цивільної безпеки.* 2019. № 2. С. 141-144.
Купчак Б.Ф. Економічна безпека підприємництва: суть та умови виникнення. *Науковий вісник Львів. держ. ун-ту внутр. справ*. Серія екон. 2019. Вип. 2. С. 334-346.
Кухонні війська в дії: як ресторанний бізнес підтримує українців під час війни. URL: https://insider.ua/ua/kuhonni-viyska-u-dii-yakrestoranniy-biznes-pidtrimue-ukrainciv-pid-chas-viyni/ (дата звернення: 10.02.2024).
Лугова В.М. Соціальна безпека як ключова підсистема безпеки під приємства. *Бізнес-інформ*. 2019. № 10. С. 69-72.
Мацьків О. О., Шах А. Є. Технічні системи безпеки готельно-ресторанних комплексів. *Вісник Львівського державного університету безпеки життєдіяльності.* 2014. №. 9. С. 150-154.
Мороз О В., Карачина Н.П., Шиян А.А. Концепція економічної безпеки сучасного підприємства: монографія. Вінниця: ВНТУ, 2019. 241 с.
Омельчук С.С. Визначення сутності поняття «економічна безпека підприємства» та його складових. *Вісник Хмельниц. нац. ун- ту. екон. науки*. 2019. Т. 1. № 6. С. 206–210.
Офіційний сайт Центру контролю якості виробництва та послуг «ATTESTOR». URL: https://atestor.ua/uk/ (дата звернення: 10.02.2024)
Парпан Т. В. Сучасний стан правового регулювання пожежної безпеки в Україні. *Право і суспільство*. 2019. №. 2. С. 225-229.
Полотай Б. Я., Жмур-Клименко Б. В. Ресторанний бізнес під час війни. *Індустрія туризму і гостинності в Центральній та Східній Європі*. 2022. №. 7. С. 37-42.
Поняття про техніку безпеки. URL: https://buklib.net/books/35189/ (дата звернення: 12.02.2024).
Постова В. В. Якість продукції та послуг як об'єкт управління на підприємствах ресторанного господарства. *Економіка та суспільство.* 2022. №. 41. С. 23-31. DOI: https://doi.org/10.32782/2524-0072/2022-41-49
Процак К., Передрій М. Ресторанний бізнес в умовах кризи: проблеми та напрямки розвитку. *Економіка та суспільство*. 2022. №. 44. DOI: https://doi.org/10.32782/2524-0072/2022-44-49
Ресторани під час війни. URL: https://kp.ua/ua/economics/a658958-olhanasonova-restorani-pid-chas-vijni-tse-psikholohichnij-pritulok (дата звернення: 10.02.2024).
Рібун М.В. Безпека підприємств готельного бізнесу як об'єкт теоретичного дослідження. *Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна*. 2019. Вип. 1. С. 304-313. URL: http://nbuv.gov.ua/UJRN/Nvldu_e_2019_1_40 (дата звернення: 25.01.2024).
Русавська В. А., Чеботаєва Т. С. Застосування принципів системи НАССР для вдосконалення системи управління якістю продукції та послуг у ресторанному бізнесі України. *Підприємництво і торгівля*. 2021. №. 28. С. 78-83.
Стельмащук Н.А. Управління економічною безпекою розвитку підприємства. *Сталий розвиток економіки*. 2019. № 3. С. 68–74.
Тітомир Л., Власюк К. Переваги системи НАССР в ресторанному бізнесі. *Економіка та суспільство*. 2022. №. 45. DOI: https://doi.org/10.32782/2524-0072/2022-45-74
Що потрібно знати про основні принципи системи НАССР. URL: https://cherkconsumer.gov.ua/novyny/731-shcho-potribno-znati-pro-osnovni-printsipi-sisteminassr (дата звернення: 10.02.2024).
Щодо запровадження НАССР у закладах громадського харчування. URL: https://dpss.gov.ua/bezpechnist-harchovihproduktiv-ta-veterinarna-medicina/sistema-haccp (дата звернення: 10.02.2024).
Як український ресторанний бізнес адаптується до викликів війни: дослідження. URL: https://business.rayon.in.ua/news/547964-yak-ukrainskiy-restoranniy-biznes-adaptuetsya-doviklikiv-viyni-doslidzhennya (дата звернення 11.02.2024).

Moisiienko A. V. Threats to economic security business hotel and restaurant business management. *Bulletin of the Cherkasy Bohdan Khmelnytsky National University. Economic Sciences.* 2019. №. 1. Pp. 345-352

DOI 10.5281/zenodo.10821959
UDC 351.862.4(477):004

CHAPTER 13.
THEORETICAL BASIS OF THE INFORMATION AND ANALYTICAL SUPPORT DEVELOPMENT OF THE SECURITY FORCES OF UKRAINE: ASPECTS OF STATE GOVERNANCE

Kostyantyn SPORYSHEV
candidate of technical sciences, assistant professor
National Academy of the National Guard of Ukraine,
(3, Maidan Zahisnykyv Ukrainy, Kharkiv, 61001, Ukraine)
spor_kos@ukr.net
https://orcid.org/0000-0003-4737-9698

Abstract. The process of organizational design of information and analytical support in Ukraine was initiated in the early 90s. Analytical services (units) were created in all nodes of the information infrastructure, that is, in all spheres of activity where large information flows were concentrated and processed for the purpose of making socially significant management decisions. That is why information and analytical services (units) began to be created in the structures of state and military administration bodies, in ministries and departments, in mass media bodies, in the field of business, in political parties and movements. A common distinguishing feature of these services is their organic entry into the respective spheres of activity, functional and organizational symbiosis with their social institutions, specific organizations and management bodies.

An important component that determines the capabilities of the management system are its resources, which consist of resources for hierarchical search and distribution of information, that is, the system that includes information sources. In addition, the capabilities of the control system are affected by the resources of the system of active influence on the enemy during the implementation of decisions. They include information resources containing the capabilities of the security forces. Thus, the first contradiction that has developed in management systems is the contradiction between the objective growth of information volumes and the inability of management bodies to process the provided information in a timely manner to make rational decisions. Today, the main task for scientists, the military-industrial complex of any country is to find ways to automatically support creative processes in the activities of military management bodies, especially for decision-making in the current time of management of service-combat actions.

In the system of military management, a second contradiction arose - between the growth of the role of organizational tasks and functions of management bodies in the system and the insufficient development of scientific methods of preparation and decision-making for them in conditions of uncertainty. That is why there is a need to develop the foundations of the decision-making theory for military management bodies, which will enable military cybernetics scientists to create algorithms for management processes and decision-making processes at the system level.

Objectively, a third contradiction also arises - between the need to apply new decision-making methods, based on reducing the impact of uncertainty on the effectiveness of decisions, and the lack of appropriate technologies for substantiating proposals for a decision.

Key words: effectiveness of state administration, modern challenges, information and analytical support, conceptual foundations of state administration, service and combat activity, security forces.

Introduction. The civilization processes of our time generate intense information flows, information bursts that reflect their interaction at the information level. In the modern world permeated by information communications, this interaction is gaining global speed. Any information disturbance is introduced into the global and national information space with great speed, gaining the ability to actively influence the life of an individual, nations, states, and the entire world community. In connection with these phenomena, in the 70s and 80s of the 20th century, a new information regime was in demand - the regime of information analytics, which was implemented mainly on the scale of sectors of the world information space. The process of organizing IAS in Ukraine was initiated in the early 90s. Analytical services (units) were created in all nodes of the information infrastructure, i.e. in all spheres of activity where large information flows were concentrated and processed in order to make socially significant management decisions. That is why information-analytical services (units) began to be created in the structures of state and military authorities, in ministries and departments, in the media, in business, and in political parties and movements. A common distinguishing feature of these services is their organic entry into the relevant spheres of activity, functional and organizational symbiosis with their social institutions, specific organizations and governing bodies (GBs). Information-analytical activity, like any infrastructure industry, is characterized by two parameters: certain instrumental characteristics (technological knowledge, methods and tools of this activity) and subject (sectoral) knowledge of the sphere in which this infrastructure activity is included.

The use of information and analytical support (IAS) in decision-making support processes during the performance of service and combat missions of security forces is

becoming an extremely important aspect. Modern requirements for improving the efficiency of IAS require the introduction of advanced IT technologies *(Tkachenko V.I., Smirnov E.B., Drobakha G.A., Bilchuk V.M., Tristan A.V., 2008)*. For the further development of IAS of the security forces, it is planned to create and use modern information and analytical systems. The main task of these systems is to collect, accumulate, store, dynamically display and multidimensionally analyze accumulated and current data, as well as analyze trends, model and predict the results of various management decisions. At the moment, IAS can act as an effective tool for supporting management decisions, providing users with all the necessary information visually and promptly to analyze the state of affairs and make management decisions.

Currently, the system of the Ministry of Internal Affairs of Ukraine has virtually no IAS whose services can constructively support effective decision-making in planning and performing its operational tasks *(Bochkovyi, O.V., 2010)*, using all the necessary information sources. Ensuring the efficiency of management, especially in the case of rapid complication of the operational situation with the use of security forces, is a key task of military command and control bodies. This process is optimized through the introduction of modern information and analytical systems (IAS) based on a transdisciplinary approach *(Tkachenko V.I., Smirnov E.B., Drobakha G.A., Bilchuk V.M., Tristan A.V., 2008).*

Expert analytical activities that support decision-making with the use of security forces are based on information resources that include not only the nomenclature and characteristics of service and combat tasks, but also a set of messages and information from various sources, including the media. However, without proper analytical services, these resources remain a passive component of the information space of the Ukrainian security forces. Insufficient processing of these resources limits their integration and significantly reduces the efficiency of their use, which is noted in the current state of information and analytical support of the security forces.

To optimize the processing of such information, it is necessary to have appropriate software and information software that is capable of implementing intelligent cognitive services for integrated analytical processing of the narrative of service-combat tasks. This should consider the content of mass media, interact with linguistic-semantic and conceptual content analysis, and provide a structural display of the results for use in all system components, such as properties, functional characteristics, and intersystem connections.

The analysis of the automation of decision support processes for the use of security forces allowed us to determine that in each of the areas separate components of information systems have been created, but they are heterogeneous in terms of time of creation, degree of completion, technologies used, scope of process coverage, scope of deployment and data filling, as

well as the possibility of integration into a single information environment based on cognitive processing of information resources, taking into account the principles and standards of the European Union and NATO *(Tkachenko V.I., Smirnov E.B., Drobakha G.A., Bilchuk V.M., Tristan A.V., 2008)*.

The state of the information and analytical infrastructure aimed at meeting the needs of the leadership of the security forces does not meet the current challenges in supporting decision-making on the use of force. The integration of information systems in certain areas is absent or fragmented, and does not consider modern requirements for consolidation, which leads to duplication and insufficient reliability and completeness of information on the integrated management of the processes of performing service and combat missions in general.

The following issues are also unresolved: lack of uniform methodological, scientific, technical and organizational principles and reasonable approaches to the creation of IAS and the introduction of modern cognitive information technologies; lack of uniform data exchange standards between information systems to ensure interoperability (interoperability); insufficient development of information protection issues (information resources); insufficient branching of information and telecommunication networks and fast data transmission channels; organizational dispersion and functional disconnection of existing information systems; the imperfection and incompleteness of the regulatory and legal regulation of the life cycle of information systems in the Ministry of Internal Affairs and Communications of Ukraine.

The solution to these problems, which are characterized by the IAS inconsistency, involves the development of a set of targeted, time- and scope-coordinated resource provision measures. These measures should be aimed at creating a modern intelligent IAS in the interests of the security forces on the basis of component-based creation of aggregated cognitive decision support services, and in the future, the formation of a unified information infrastructure of the security forces.

This will ensure the necessary level of efficiency, reliability and completeness of information required for making managerial decisions on the operational use of forces.

Analysis and monitoring of information threats to the state security of Ukraine.

Threats to information security of the national security management system include:

- disclosure of information resources; violation of their integrity;
- failure of the equipment itself.

Due to their number, according to the general classification of threats to national security, threats to information security are distinguished by different criteria. By sources of origin:

- natural origin (mass destruction of communication channels due to natural disasters);

- man-made (accidents on engineering networks and life support facilities, accidents of the main servers of the national security management system, etc;)

- anthropogenic (erroneous launch of a programme, (un)intentional installation of bookmarks due to non-compliance with Internet security rules, etc.)

By the nature of implementation:

- real (activation of destabilisation pathways is inevitable and not limited by time and space);

- Potential (destabilisation is possible under certain conditions of the environment in which public authorities operate);

- Fulfilled (threats have been implemented);

- Imaginary (conditional or similar to existing threats, but not real).

By the degree of hypothetical damage:

- threat (obvious or potential actions that complicate or make impossible the realisation of national interests in the information sphere and pose a danger to the national security management system, life support of its systemic elements);

- danger (direct destabilisation of the functioning of the national security management system).

Probability of implementation:

- probable (if a certain set of conditions is met, they will definitely occur, for example, the announcement of an attack on information resources, which precedes the attack itself);

- impossible (will never occur if a certain set of conditions is met, are mostly declarative in nature, not backed by a real or even potential ability to implement the declared intentions, and are mostly intimidating);

- random (under a certain set of conditions, they occur in different ways and are analysed using methods of operations research, in particular probability theory and game theory, which study patterns in random phenomena).

By the level of determinism:

- random (threats that may or may not occur - threats by hackers to destabilise the information system of the authorities),

- natural (threats of a stable, recurring nature caused by the objective conditions of existence and development of the information security system - numerous hacker attacks on the official websites of the FBI, CIA of the United States) *(Bogush, V. M., Krivutsa, V. G., Kudin, A. M., 2004).*

This list, of course, can be continued, but the following conclusion is obvious. Thus, the concept of threats is considered mainly in an abstract or simplified way, sometimes narrowly, detached from the context of the concept of "information security" and almost not related to the

context of the generic concept of "threat". We consider threats to Ukraine's information security as determining factors that cause and generate negative phenomena that encroach on national interests in the information sphere, organisation and functioning of the national information space in general. They have or may have a wide-ranging significance, being associated with risks and dangers in other areas. Thus, the legislation of Ukraine regulates threats to the national security of Ukraine at the current stage of development of our society and state in the foreign policy sphere, in the sphere of state security, in the military sphere and in the sphere of security of the state border of Ukraine, in the domestic political sphere, in the economic sphere, in the social and humanitarian spheres, in the scientific and technological sphere, in the sphere of civil protection, in the environmental sphere, in the information sphere. The threats to information security, as well as to the state sovereignty and territorial integrity of the state of Ukraine, are directly determined by such threats as claims from other states, globalisation of world relations and concentration of levers of influence on world processes in the hands of individuals or groups, manifestations of separatism and attempts to autonomise certain regions of Ukraine on ethnic grounds. All other threats to the national security of Ukraine may not directly pose a danger of encroachment, but to one degree or another undermine these fundamental values of the state and society *(Nosach A.V., 2019)*. It should be emphasised that threats to the information security of the state go beyond the geographical borders of states, encroach on the national information space, but may have cross-border or global negative consequences. The need for further study and development of a clear concept of "threat" is urgent and should be aimed at forming an effective and realistic system of monitoring and management of threats and other risks to the information security of the state. In order to prevent and counteract existing and possible threats to information security, the strategic task of the state is to create and operate a mechanism for ensuring information security. It involves consistent systematic activity, a set of measures and state and legal institutions designed to guarantee the unimpeded realisation of the national interests of the state in the information sphere, the relevant interests of individuals and society, prevention of information conflicts and their prompt overcoming. Given the active globalisation of information and communication networks, it is important not only for states but also for international organisations to engage in cooperation in countering various types of information aggression *(Kormych, B. A., 2008), (Tkachuk, P.P., Gula, R.V., Sivak, O.I., Shchurko, O.M., & Shemchuk, V.V., 2015), (Shemchuk V., 2020).*

Information and analytical technologies in modern public administration

Today, the world is witnessing a rapid development of information technologies (IT) and their penetration into all spheres of human activity: social, economic, political, military, etc. The main

features of the revolution in information and communications in military affairs at the present stage include *(Gorodnov, V.P., Drobakha, G.A., Yermoshin, M.O., Smirnov, E.B., Tkachenko, V.I., 2004)*:

- globalisation of information processes in the armies of the world's leading countries;

- miniaturisation of the element base of computer equipment and facilitation of its integration with weapons samples;

- increasing reliability and mobility of computer networks used as a material basis for building various military information systems.

The main strategic goals of the development of the information society in Ukraine *(Matsko O. Y., Mykus S. A., Solonnikov V. H., 2021)*:

- accelerating the development and implementation of the latest competitive IT in all spheres of public life, including the Ukrainian economy and the activities of state authorities and local self-government bodies;

- development of the national information infrastructure and its integration with the global infrastructure;

- creating nationwide information systems, primarily in the areas of healthcare, education, science, culture, and environmental protection;

- improving the state of information security in the context of using the latest IT.

All of the above also leads to significant changes in military affairs:

- New concepts of military conflicts are being developed, especially the concept of "non-contact warfare",

- forms and methods of using troops are being improved.

Modern military conflicts have acquired specific features (determination to achieve political goals, focus on paralysis of state military management systems and critical infrastructure of the opposing state, dynamism, rapidity, high technological sophistication of the means used);

- automated systems of command and control of troops and weapons are being improved (with the latter clearly showing changes in the transition to the development and creation of automatic weapons control systems);

- high-precision weapons are being improved, which, due to their entry into the information environment of the "combat space", can receive certain adjustments even after launch;

- intelligence means are being improved, with certain changes in the expansion of their use, along with the space and unmanned reconnaissance means that have already been transformed into traditional means, various sensors and sensors that can operate autonomously for a long time and be at sufficiently large distances.

Today, we can say that there has been a widening of the continuum of dimensions in which armed struggle can be conducted - it can be stated that it is conducted not only in the traditional dimensions of "space-time" but also in the "information dimension" *(Gorodnov, V.P., Drobakha, G.A., Yermoshin, M.O., Smirnov, E.B., Tkachenko, V.I., 2004)*.

The analysis allows us to define quite clearly the following areas of IT application in modern armed struggle;

- use of IT in troop management systems;
- use of IT in weapons control systems;
- use of IT as a weapon;
- use of IT as a basis for structural and functional transformation of the armed forces and development of new concepts of conflict management and forms of employment of troops *(Matsko O. Y., Mykus S. A., Solonnikov V. H., 2021).*

It is the desire to achieve information superiority over the enemy and the use of the latest IT in command and control systems that has led to a certain dependence of state and military authorities on the reliable functioning of information systems. Information superiority is a tool that enables commanders to use widely dispersed formations of diverse forces in decisive operations, increase troop protection and deploy groups that are best suited to the task, as well as to provide flexible and targeted logistics support. Gaining and maintaining information superiority involves taking measures against the command and control and decision-making systems, as well as against the enemy's computer and information networks and systems. Thus, the latest IT is now turning into a systemic factor in modern armed struggle. Thanks to their use, the number of scenarios for unleashing and conducting armed conflicts with detailed planning and forecasting of their consequences in all spheres (political, economic, military, etc.) is significantly expanding. Thus, the use of IT makes it possible to create new systems and forms of armed struggle with fundamentally new properties. In other words, IT not only enables better collection, analysis, processing, interpretation and presentation of data, but also, due to its systemic capacity, opens up additional opportunities for the development and improvement of theoretical and experimental research methods in the field of military control automation and the creation of promising and improvement of existing models of weapons and military equipment. For a deeper understanding of this system-forming process, which leads to the creation of a new quality, future scientists need to consider the content of the definition of the concept of system from a dialectical perspective and to get acquainted with the basic provisions of the theory of complex systems. This will make it possible to make fuller use of IT capabilities to improve the effectiveness of weapons and military equipment, command and control systems and weapons control systems as complex military systems. In addition, there are new opportunities to open a qualitatively

new stage in the development of military art - the transition from command and control of troops during an armed conflict to conflict management in general.

According to military experts, information and analytical support (IAS) is considered a type of support for the security and defence forces, as well as logistical, combat, medical and other types of support.

The origin of IAS is associated with the development of computing technology. The widespread use of computers has had a significant impact on the IAS system. However, analytical work was carried out in the relevant headquarters before. It is necessary to consider the IAS system within the military command and control system.

The chronology of the development of the theory of organisational systems management is shown in Figure 1.1.

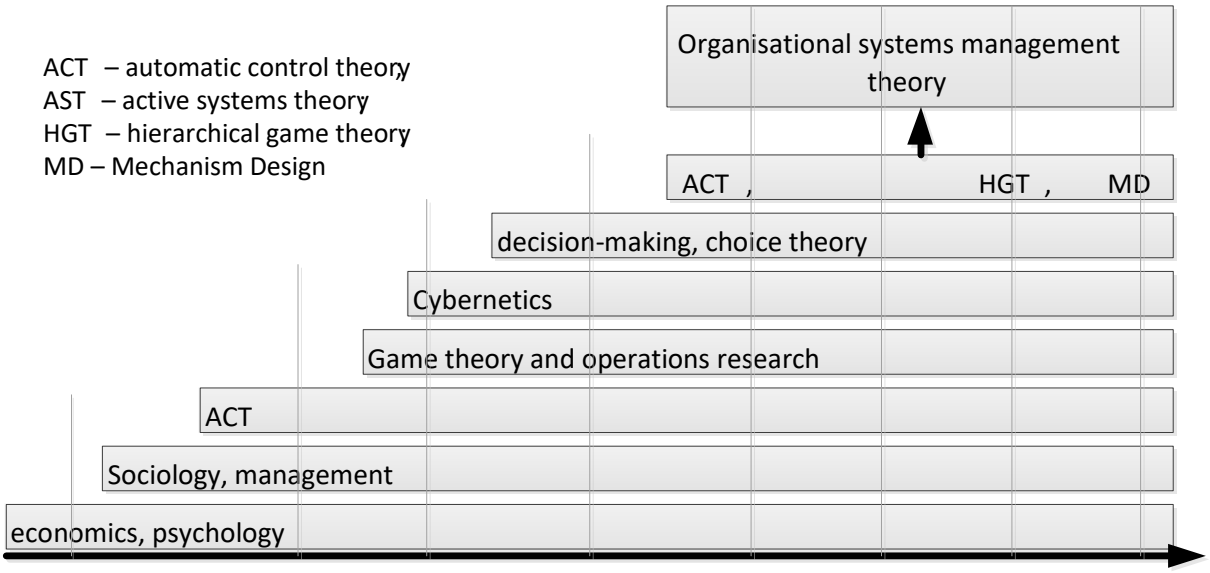


Figure 1.1 - Basics of the origin of management theory

The information-analytical system for management processes (IASMP) forms the basis of the ACS and includes: an information support subsystem and a decision support subsystem. Depending on the types of information processed in the IASMP, the decision support system uses appropriate information processing algorithms.

The first type of information is that describing probabilistic events, the parameters and indicators of which can be described by known laws of distribution of a random variable. The second type includes information that is non-stochastic in nature, i.e. when the parameters and indicators of events are described by the methods of fuzzy set theory. The third type of information is deterministic and is processed using conventional mathematical methods of operations research.

An important component that determines the capabilities of a control system is its resources, which consist of the resources of hierarchical search and distribution of information, i.e. the system that includes information sources. In addition, the capabilities of the control system are influenced by the resources of the system of active influence on the enemy during the implementation of decisions. They include information resources that contain the capabilities of the security forces.

Moreover, these information resources are used in the management system in case of their deployment and inclusion in the overall structure of the management system. Such a command and control system with an appropriate information and analytical system to support management processes is adaptive to the type of incoming information, to the state of the situation and forces monitored in the current time, and allows making decisions in the rhythm of the work of the headquarters, which is the main purpose of this command and control system [47].

World practice shows that the information burden on command and control bodies is increasing significantly.

For example, the well-known EMC Corporation provides research results on the growth of information created and used in the global society.

For example, in 2006, 161 exabytes of digital information were created and copied. The period of unprecedented information growth continues. This figure is approximately 3 million times the amount of information stored in all books ever written. According to the IDC (International Data Corporation), the amount of information created during 2010 will increase more than six fold to 988 exabytes, with an overall annual growth rate of 57%.

The information burden on military command and control bodies is growing in the same proportion. In a few years' time, decision-making without modern information and analytical support will be problematic for command and control bodies.

Thus, the first contradiction in command and control systems is the contradiction between the objective growth of information and the inability of command and control bodies to process the information provided in a timely manner to make rational decisions.

Today, the main task for scientists and the military-industrial complex of any country is to find ways to automate creative processes in the activities of military command and control bodies, especially for decision-making in the current time of combat operations management.

There is a second contradiction in the military command and control system - between the growing role of organisational tasks and functions of command and control bodies and the lack of development of scientific methods for them to prepare and make decisions in conditions of uncertainty.

That is why there is a need to develop the basics of decision-making theory for military command and control bodies, which will enable military cybernetics scientists to create algorithms for management and decision-making processes at the system level.

The concept of information and analytical support is a category of management theory. The functions of IASMP should also include support for weapons control processes at the tactical level of command. An important task of the IASMP is to support the processes of preparation and decision-making by the management bodies of the security forces of Ukraine *(Matsko O. Y., Mykus S. A., Solonnikov V. H., 2021).*

It should be noted that the technology of preparation and decision-making in the military sphere has not changed much over the years (almost since the Second World War), which significantly affects not only the quality of real-time combat management and comprehensive support, but also the quality of the processes of daily life of a military organization. At the same time, the existing methods of preparation and decision-making in difficult conditions negatively affect the coherence of cooperation between military bodies and public administration bodies, which are already implementing new technologies and setting appropriate requirements for decisions made in the military sphere.

Obviously, there is a third contradiction - between the need to apply new decision-making methods based on reducing the impact of uncertainty on the effectiveness of decisions and the lack of appropriate technologies for justifying decision proposals.

Due to the formalization of the processes of taking into account significant factors that are not clearly described by the management bodies and affect the content of the plan, the insufficient reliability of mutually independent alternatives with their respective number gives the right to consider the final reliability of the result greater than for each alternative separately, which is supported by taking into account the physical content of the factors themselves.

If we consider uncertainty in decision-making processes as the absence (or inadequacy) of necessary information, then using information theory, we can calculate the level of uncertainty (the value of information entropy) through the membership function of fuzzy sets and obtain the desired threshold of reliability (sufficiency of information volume) deemed adequate for decision-making. This approach enhances the effectiveness of decision-making during combat operations.

In addition to technologies for preparing and making decisions in modern conditions, the quality of command and control of troops (forces) is influenced by the structure of the information and analytical system, its integrity, the quality of support for the processes of managing security forces, and the content and completeness of the data being analyzed. Considering that the basis of management processes are decisions made by the management bodies, the information and analytical

system primarily supports the processes of preparation and decision-making. The quality of decisions will determine the results of the functioning of not only the management system itself, but also other processes related to assigned tasks.

The main problematic issues of information and analytical support for the management bodies of security forces at this stage include: insufficient development of the regulatory framework in the security forces of Ukraine regarding the creation of information resources and products, provision of information services, and functioning of the information and analytical support system of management bodies as a whole; absence of a system of interconnected information and analytical bodies of security forces, functionally, technologically, and technically linked; lack of a unified system for classifying and encoding information in the security forces of Ukraine; insufficient development of general information resources in the security forces of Ukraine and the absence of an integrated database, which should become an element of the national information structure; the necessity of using certified systemic software and mathematical support that has already proven itself in practical activities; absence of certified means of information security; the absence of a clearly defined complex of specialized software and mathematical support for information activities; the necessity of training specialists to work in modern information and analytical systems; insufficient funding; lack of a comprehensive approach in organizing research to address the problems of creating the information support system for the security forces of Ukraine. Currently, insufficient research is being conducted in such areas as improving the regulatory framework, enhancing the system of information and analytical units, creating a comprehensive information protection system, developing systemic requirements for the certification of information technology and information and telecommunication systems in the security forces of Ukraine.

Simulation models and simulations of military or combat operations are used to analyze and model various aspects of military operations. These tools allow for virtual training, strategy exploration, evaluation and analysis of options, and improvement of tactical and strategic decisions. Here are some typical simulation models and simulations in this context:

JTLS (Joint Theater Level Simulation) is an example of a large-scale simulation system for analysis and training at the military theater level.

VBS3 (Virtual Battlespace 3) is a simulator designed to model various aspects of combat and military operations. It is used for training, analysis and study of tactical decisions.

CMANO (Command: Modern Air/Naval Operations) is a simulation game designed to model modern air and naval operations. It allows you to analyze tactical scenarios and strategies.

SIMDIS (Simulation Display System) is used to visualize simulation data and can be used to analyze the movement of military units, model atmospheric and terrain conditions, etc.

ACE (Advanced Computerized Environment) is a platform for creating simulation models and simulations of military operations. It provides opportunities for training and research.

DI-Guy is used to model the appearance and movement of military personnel in various scenarios.

These tools help military professionals analyze various scenarios, improve strategies, train military personnel, and study the impact of various factors on the outcome of military operations. In addition, they can be used to study new technologies and tactics in the military sphere.

Strategic and tactical military decision-making requires careful planning, analysis, and effective resource management. There are different approaches to this process, and they may differ depending on the specific situation, methodology and area of military operations. These are some common approaches to strategic and tactical military decision-making:

- using a system approach to consider the entire situation of military operations, taking into account the various interrelationships and the influence of various factors;

- assessing the internal strengths and weaknesses of own forces and those of the enemy to develop strategies that maximize the advantages and compensate for the disadvantages;

- taking into account geopolitical factors, such as geographical location, resources and geostrategic importance of regions;

- assessing potential threats and opportunities arising from the external environment to formulate security and defense strategies.

- SWOT analysis (Strengths, Weaknesses, Opportunities, Threats). The use of SWOT analysis to identify strategic advantages, disadvantages and opportunities, as well as to identify potential threats;

- development of different courses of action, taking into account various possible scenarios and determining the most optimal one;

- ability to quickly adapt to changes in the military environment and respond to unforeseen circumstances;

- leadership and teamwork to effectively coordinate actions on the battlefield;

- use of modern technologies to increase efficiency and ensure an advantage in battle.

Military decision-making requires a multifactorial approach and a deep understanding of one's own capabilities, strategic goals, and tactical circumstances. Each stage of military operations requires careful analysis and development of effective strategies to achieve the set goals.

MDMP is an acronym for Military Decision-Making Process. It is a standard approach to strategic and tactical military decision-making used in the armies of numerous countries. The main goal of MDMP is to the systematization and standardization of the military planning and decision-

making process. It takes into account numerous aspects to ensure the efficiency and success of military operations.

The main stages of the MDMP include:

Mission Analysis is the first stage in which the commander analyzes the mission, gathers information about the situation, and assesses the initial conditions;

Course of Action Development. This stage generates possible courses of action to accomplish the mission. Each course of action is carefully designed and evaluated, taking into account various factors such as enemy forces, terrain, time, and resources.

Course of Action Analysis. The commander and his staff evaluate each course of action by comparing them according to various criteria, such as effectiveness, risk, and cost.

Course of Action Selection. The commander chooses the most appropriate course of action, taking into account the evaluations and analysis conducted in the previous stages.

Orders Production. At this stage, an order is generated that includes all the necessary details for implementing the chosen course of action, including tasks for departments, resources, and communications.

Execution. At this stage, the execution of the order begins, and the commander observes the development of the situation, making the necessary changes to the execution of tasks.

The MDMP is defined by structure, discipline, and decision-making orientation in a military context. Its main purpose is to provide staffs and commanders with effective tools for planning and managing military operations.

JTLS (Joint Theater Level Simulation) is a large-scale military computer simulation system used for training and exercises in joint operations at the theater level. This system is designed to model and analyze military operations in real-time over large areas, taking into account various aspects such as logistics, communications, fire support, reconnaissance, engineering, and others.

The main characteristics and functions of JTLS may include:

Simulation of various aspects of combat operations. Taking into account the various components of the modern combat environment, including land, air and sea forces.

Simulation of logistics aspects such as supply, transportation, maintenance, ammunition, etc.

Taking into account the capabilities of fire support, artillery, aviation and other fire systems.

Real-time simulation of communication systems and command and control structure.

Taking into account the actions of intelligence assets and information garnering.

Providing military personnel with the opportunity to use the system for training and preparation for real-life situations.

Ability to model different types of conflicts, including symmetrical and asymmetrical threats.

JTLS allows military teams and analysts to perform real-time analysis and planning, improving their decisions and strategies in a virtual military environment.

The development of military affairs for the most part is based on the analysis of experience from past wars and armed conflicts however, in modern conditions, computational experiments using various types and scales of mathematical models and simulation complexes are becoming increasingly widespread. With their help, it is possible to predict the nature, forms, and types of armed conflicts, as well as to test new weapons, new technologies for organizing and conducting military operations.

Today, there are various trends in the application of the mathematical description of armed confrontation, in particular, a mathematical description based on the comparison of combat capabilities, logical and analytical methods characterized by the representation of real processes and systems in the form of explicit functional dependencies (scenarios, stages of decisive rules), simulation methods, which describe the apparatus for making more frequent decisions with an element of probability (target hit/not hit, detected/not detected, etc.). However, for processes and systems that have a complex nature of action, such as the processes of armed struggle, in the absence of the possibility of mathematical formalization that provides an analytical solution to the problem, the only approach to research is to use simulation modeling methods.

In the process of designing models of armed confrontation and preparing system and software solutions, the modeling objective, its functional purpose, and the place of the model in the decision-making system are primarily taken into account. At the same time, it should be understood that the model is only a tool for staff officials and commanders and cannot ensure the development of a single correct and comprehensively justified decision in a particular situation. The model is an auxiliary tool to support the decision-making process and evaluate possible alternatives. This is due to the fact that its mathematical apparatus and algorithms cover a variety of complex processes, factors and conditions that directly affect the modeling results. Some of them are quantified, such as the combat and numerical composition of conflicting groups, types and characteristics of weapons and military equipment, resources, physical, geographical and meteorological conditions, and others.

The other part of the initial data cannot be represented in quantitative terms for objective reasons due to the fact that they belong to the cognitive sphere of a person. That is why today only formal data is taken into account in the modeling of combat operations.

Taking into account the bilateral nature of armed confrontation is the most important methodological feature of modeling. In this case, it refers to the complex processes of confrontation between two antagonistic systems that engage in not only combat but also intellectual conflict, which is envisaged by the parties' plans. Based on this, today an armed confrontation (operation, battle) is

considered not only as an armed confrontation between two antagonistic systems, but also as systems that simultaneously realize all their information, moral and combat, psychological and moral and technical potential, which is taken into account in the two decisions of the conflicting parties. That is, the intellectual confrontation of two adversaries who implement their decisions through the prism of the actions of subordinate troops.

In this approach, it is necessary to take into account the fact that the results of hostilities should be viewed through the prism of achieving the goal and fulfilling the assigned combat tasks by their troops, despite the fact that this structure reproduces the symmetry of the parties' actions, and the enemy is viewed as an external source of random and unfavorable actions that force the search for new solutions in accordance with the rapidly changing situation.

In this structure, combat operations are modeled at three levels of command.

The first level provides modeling for the decision-making of the commander of the operational unit (HICON).

The second level covers the decision-making processes and tasking of the tactical command and control (PTA).

The third level is the level of task performers, i.e. directly subordinate units (LOWCON), where the practical implementation of decisions of the two higher levels is modeled. In essence, the third level is a set of separate models of combat operations of different types and branches of the military and is the "physical" environment of the model, where not just an armed conflict is reproduced, but a set of all confrontations in all areas of their realization.

It should be noted that in order to ensure the flexibility of the model, taking into account the intermediate results of operational and tactical calculations and the impact of the combat situation, human intervention in the modeling process is provided through specific procedures. This allows to take into account new data arising from the development of the situation, obtain intermediate and final indicators, change the modeling conditions, clarify and evaluate the impact of various factors on the preliminary plan. Under these conditions, the modeling process is programmed discretely, in stages and with step-by-step recording of the state and position of the parties' forces and means. At each stage, it is possible to refine the data and obtain various options for action.

It should be noted that nowadays almost all existing models:

- do not take into account changes in the nature and content of modern armed conflict;

- do not "feel" all the variety of forms and methods of operational and combat employment of troops;

- do not take into account informal initial data, such as the military art of commanders, their tactical "literacy", motivation and moral and psychological preparation of personnel;

- do not answer the question of what to do to get the desired result. The use of modern models to draw up the most rational plan requires consideration of a large number of alternatives and is suitable only for the stage of advance preparation for combat operations.

Combat models of aggregated forces are widely used in the defense departments of the world's leading countries to simulate military operations during training and for research purposes to improve the validity of plans and programs for the creation, development and employment of armed forces and decision support.

The theoretical basis of such models are systems of deterministic differential equations. Such well-known differential equations are the Lanchester models.

The JCATS simulation system, in terms of using the mathematical apparatus for the formalized description of the processes of armed struggle, is a hierarchical model *(Taylor James G, 2001)*, which consists of two levels:

Level 1 - a detailed description of interaction at the level of individual objects using the method of statistical testing (Monte Carlo).

The following are taken into account: composition and tactical and technical characteristics of weapons, surveillance equipment, type of ammunition and its destructive capability, dimensions of the object, range of possible speeds of movement of objects; influence of terrain characteristics, weather conditions, season, time of day, and other factors (smoke, noise, river flow, depth of water obstacles and nature of the bottom, replenishment of stocks, restoration of forces and means, fatigue of personnel, level of their training, use of weapons of mass destruction, impact of the consequences of shooting, natural disaster, etc.)

Level 2 - description of interaction at the organizational unit level (Unit Level), which is defined as aggregate systems, using Lanchester's differential equations. Aggregate systems are created from the level of the squad and higher one.

To summarize, the JCATS system utilizes a hierarchical approach, where at the lower level, the interaction of individual combat units is simulated using the Monte Carlo method, at the intermediate level, interaction is described by Markov models, and at the top (aggregated, deterministic) level, Lanchester's differential equations are used. Above these models, introducing control parameters into them allows for the construction of management tasks in terms of controlled dynamic systems, differential games, or repeated games.

Information about the internal details and mathematical aspects of such systems is often classified and not disclosed for security reasons.

However, simulation modeling, including JCATS, typically uses a variety of mathematical models to describe movement, interaction, and decision-making in military scenarios. Some common aspects that mathematical models may include are:

Kinematics and Dynamics. Mathematical models that describe the movement and interaction of objects in space, such as vehicles, military units, etc.

Weapons and Fire Support. Models for determining the effectiveness and impact of various types of weapons, as well as algorithms for modeling fire support.

Logistics and Supply. Mathematical models to describe logistics operations such as supply, transportation, maintenance, etc.

Intelligence and Positioning. Models for reconnaissance operations and determining the positions of enemy and own forces.

Decision-making algorithms. Mathematical models for algorithms that determine the actions and reactions of forces in various scenarios.

Communications and Command:

Models to describe real-time communication and command and control systems.

These mathematical models and algorithms allow the simulation system to create a virtual military environment to study and train various military scenarios.

Genesis of Information and Analytical Support provided to the security forces of Ukraine for their assigned tasks.

Information and analytical support (IAS) for the security forces of Ukraine is an important component of the country's modern national security system. The development of this sphere in Ukraine took place in the context of challenges and threats arising from geopolitical events, changes in the technological space and the need to adapt to international standards.

The post-independence period (1991-2000). In the first years after becoming independent in 1991, Ukraine faced numerous challenges and tasks related to the formation of its own security and defense system. During this period, information and analytical support (IAS) for the security forces of Ukraine was not yet a properly developed industry, and it was going through the stages of formation and organizational development. During this period, information and analytical support consisted mainly of outdated methods of information analysis.

The main characteristics of the IAS in the first years after becoming independent:

This period is characterized by new challenges and the need for a new security system. The collapse of the Soviet Union led to the creation of an independent security system for the newly formed state. This involved the formation of its own armed forces, intelligence and other security services. There was a lack of experience and resources. Ukraine had limited resources and equipment

to implement its own IAS system. Knowledge and experience in the field of information security was limited, and the country faced the task of recreating its own defense and security structures. In the first years of independence, intelligence played a special role in ensuring information security. Special services focused on gathering and analyzing information about external and internal threats. At the same time, there were traditional methods of information analysis. Due to the fact that modern technologies were not yet widely implemented, information and analytical support used traditional methods of gathering and processing information. One of the negative factors of this period was the absence of standardization. During the period of formation of independence, the absence of standardization in the field of information and analytical support of the security forces made it difficult to coordinate and exchange information between different structures.

During the first years of independence, the organizational structure and strategy of the security forces were changed, which affected the development of information and analytical support. This period of formation was important for the further development of the IAS of the security forces of Ukraine, and over time, the country began to actively adapt and implement modern technologies to improve its information security capabilities.

The period of modernization (2000-2014). During this period, the supply of information and analytical tools was modernized. New technologies were introduced, including automated data collection and analysis systems. However, the development wasn't identical due to financial difficulties and other factors. During this period, the country improved its information and analytical systems, responding to modern challenges and taking into account the experience of other countries. The main aspects of this period include:

During this period, Ukraine created new structures and units aimed at providing information to the security forces. The creation of specialized agencies responsible for analyzing and processing information improved the IAS system. The growth of technological development has resulted in the modernization of IAS technical support. The use of computer technologies and software for information processing and analysis became more widespread. During this period, much attention was paid to the development of analytics and big data processing systems. This allowed performing a more accurate and quicker analysis of information, which was important for rapid decision-makingIn the face of growing interest in artificial intelligence, security forces have begun to implement it to automate some aspects of analysis and decision-making. This was an important step in the development of intelligent IAS systems. Considering the growing number of cyber threats and cyber attacks, the focus was on improving information security. The development and implementation of cyber defense has become an important element of IAS. An important component of the modernization was the professional development of information security and analytics

specialists. This included staff training in the latest techniques and technologies. The mentioned period was essential for improving the capabilities of the Ukrainian security forces in the field of information and analytical support, which was a complete response to the challenges of the present and preparation for further development of the security and defense systems.

Situation in the East of Ukraine (since 2014). The events that happened in eastern Ukraine and the annexation of Crimea by the Russian Federation since 2014 have determined the need for rapid development of information and analytical support (IAS) for the security forces of Ukraine. These events have created new challenges and threats to national security, as well as the need to have an effective system of analysis and distribution of information for rapid decision-making. The main aspects of this period include:

The Russian Federation actively used information and psychological methods to influence the situation in Ukraine. Information warfare, disinformation and cyber attacks became important aspects that required improvement of the IAS system for effective detection and response. The conflict required the processing of a large amount of information coming from various sources, including intelligence, open source data and others. The IAS system had to provide fast and efficient analytical processing of this information. The development of cyber threats and cyber attacks, the application of hybrid wars, required the improvement of cybersecurity measures and the use of the latest technologies to detect and prevent attacks. One of the characteristic features of this period was the development of cyber analytics. In order to detect and analyze cyber threats, security forces needed to improve cyber analytics systems. This included analyzing large amounts of cyber data and introducing new methods of threat detection. Ukraine has established specialized headquarters and information and analytical support centers to coordinate and exchange information between various agencies and military units. Measures were taken to organize international cooperation in the field of cybersecurity and information security. Ukraine cooperated with other countries and international organizations in the field of cybersecurity and information security to share experience and receive support in defeating threats.

In general, the events in eastern Ukraine and the annexation of Crimea have determined the rapid development of information and analytical support for the security forces, making it more adapted to current threats and challenges.

The creation of new structures (since 2014). In order to improve the security and defense system, Ukraine has created new structures, including the Foreign Intelligence Service of Ukraine and other agencies that actively use information and analytical technologies to support their tasks. In connection with the implementation of strategic tasks and improvement of the security and defense system in the face of modern threats, Ukraine has created new information and analytical support

(IAS) structures. These structures are designed to improve the efficiency of the security forces and provide timely and accurate information for strategic decision-making. Some of these structures include:

Information and Analytical Department of the Ministry of Defense. It was created for centralized management and coordination of information and analytical activities in the field of defense.

Information and Analytical Center of the General Staff of the Armed Forces of Ukraine. Provides analysis of the current situation in the country and the world, development of forecasts and analytical materials for the senior military leadership.

Cyber Defense Center of the National Guard of Ukraine. It was created to ensure cybersecurity and protection against cyber threats, including important facilities and information resources.

Information and Analytical Department of the Security Service of Ukraine. Responsible for collecting, analyzing and processing information on threats to national security, internal and external intelligence.

The Department of Information and Analytical Support of the Ministry of Internal Affairs. It was created to process information on internal threats, ensure the situation in the country and support the operations of the MIA units.

Center for Information and Analytical Activities of the Foreign Intelligence Service of Ukraine. It is engaged in the collection, analysis and processing of information in the international context, intelligence and protection against external threats.

The creation of such IAS structures helped to provide Ukraine's security and defense system with modern and effective tools for analyzing information, identifying threats and responding to them in a timely manner. This is an important step in protecting national interests and ensuring the country's security in the face of current challenges and threats.

Application of the latest technologies (since 2014): As a result of technological and information developments, Ukraine's security forces have begun to implement the latest technologies to ensure efficiency, accuracy and responsiveness in information and analytical support (IAS), such as artificial intelligence, cybersecurity, big data analysis and other tools for collecting and processing information.

Security forces are using artificial intelligence to automate the process of analyzing large quantities of data, identifying patterns, and making connections. Artificial intelligence (AI) can also be used to predict situations, detect anomalies, and make automated decisions. Due to the growing number of cyber threats, security forces are improving cybersecurity measures and implementing modern means of protection against cyber attacks. This includes developing incident detection and

response systems, encrypting information, and ensuring cyber protection of critical facilities. One of the latest technologies used by security forces is big data analysis (Big Data). Through the use of big data analytics, security forces can gain a more complete and deeper understanding of complex situations, identify trends, and draw strategic conclusions. The Internet of Things (IoT) is a concept that refers to the connection of physical objects to the Internet that were not previously capable of doing so. These can be various devices, household items, technical systems, cars, electronics and other objects equipped with sensors, software and the ability to exchange data via the Internet. The main idea of IoT is to connect the real world with the Internet, where objects can interact with each other, collect and exchange data using networks and communication technologies. The introduction of IoT technologies allows collecting and processing data from various sources, which makes it easier to monitor and manage objects and resources

Computer image analysis and video analytics is a technology that has become widespread in everyday life. The use of machine learning algorithms for processing and analyzing video materials provides the ability to detect anomalies, recognize objects and events. The use of the latest innovative communication tools allows security forces to effectively exchange information in real time.

These technological innovations are designed to improve the quality and quantity of information available to security forces, making them more effective in managing and responding to modern threats.

After the events of 2014, Ukraine has been actively developing international cooperation in the field of information and analytical support (IAS), cooperating with other countries and international organizations. The purpose of this is to exchange information, introduce the latest technologies and ensure collective defense against modern threats. Some key aspects of international cooperation in this area include:

- intelligence sharing. Ukraine cooperates with partners from other countries, exchanging intelligence information on threats and actions against national security;

- participation in international organizations. Ukraine is a member of various international organizations, where it cooperates with partners to address modern challenges, including information security issues;

Ukraine is developing security partnerships with other countries, which include the exchange of experience and training on information security and IAS;

- technical assistance. Through international cooperation, Ukraine can gain access to the latest technologies and innovations in the field of information analysis and security;

- common standards and norms. Participation in international forums allows Ukraine to join the establishment and improvement of common standards and norms in the field of information security;

- joint exercises with partners facilitate interaction between different countries and increase readiness for joint response to potential threats.

This international cooperation helps Ukraine improve its information and analytical capabilities, receive support from security partners, and share experiences and best practices. It also contributes to a more unified and responsible international security system.

In general, the development of IAS of the security forces of Ukraine is determined by the requirements of the present time, security threats and the country's ability to adapt to modern challenges in the field of information security and defense.

Information and analytical support of the service and combat activities of the security forces of Ukraine is a key aspect of ensuring national security and the effectiveness of military operations. This includes collecting, analyzing and processing information from various sources to make informed decisions and perform security tasks.

The main components of information and analytical support for the service and combat activities of the security forces include:

Systematic information gathering from various sources, such as intelligence, sensors, open source information, communication signals, etc. This may include technical intelligence collection, information analysis and other methods.

Analyzing information to identify trends, assess threats, and determine strategies and tactics. This may include intelligence analysis, geospatial analysis, social media analysis, and other methods.

To ensure that commanders can easily understand the information and make decisions, the data must be processed and visualized. This may include the creation of maps, graphs, infographics and other visualization tools.

Ensuring information security is an important part of information and analytical support. Measures may include cryptographic protection, access control, and other methods to ensure the confidentiality and integrity of information.

Preparation of analytical reports and recommendations will help to make reasonable and rational decisions based on the latest information.

Permanent education and professional development of personnel is an important element, as the modern information environment is constantly changing. Training in the use of the latest technologies and methods of information analysis is essential to ensure effective service and combat activities.

These aspects help to create an integrated system that allows security forces to effectively use information to achieve their security and defense goals.

Modern informatization and communications in military affairs are characterized by numerous features that define new approaches to warfare and defense. The distinctive features of modern informatization and communication in military affairs are *(Tkachenko V.I., Smirnov E.B., Drobakha G.A., Bilchuk V.M., Tristan A.V., 2008)*:

- globalization of information processes in the armies of the leading countries of the world;

- miniaturization of the component base of computer equipment and facilitation of its integration with weapons samples;

- increasing reliability and mobility of computer networks used as the material basis for building various military information systems;

- the use of artificial intelligence (AI) and analytical systems to analyze large amounts of data, recognize patterns, make predictions, and make decisions. AI can be used for intelligence, operations planning, and threat detection;

- the development of telecommunication technologies allows for the rapid and efficient exchange of information between different levels of command and units;

- the development of telecommunication technologies allows for the rapid and efficient exchange of information between different levels of command and units;

- development of robotic unmanned reconnaissance and high-precision strike systems;

- use of geolocation systems and geoinformation technologies for operations, force deployment and route planning;

- ensuring compatibility and interaction between different systems and platforms (interoperability) to ensure effective command and control; and

- measures to protect military information from unauthorized access, cyber attacks and other threats.

The main strategic goals of the information society development in Ukraine *(Matsko O. Y., Mykus S. A., Solonnikov V. H., 2021)*:

- accelerating the development and implementation of the latest competitive IT in all spheres of public life, in particular in the economy of Ukraine and in the activities of public authorities and local governments;

- development of the national information infrastructure and its integration with the global infrastructure;

- creation of national information systems, primarily in the areas of healthcare, education, science, culture, and environmental protection;

- improving the state of information security in the context of using the latest IT.

Modern military conflicts have acquired specific features (determination to achieve political goals, focus on paralyzing the systems of state military administration and critical infrastructure of the opposing state, dynamism, transience, high technological sophistication of the means used). These features include *(Tkachenko V.I., Smirnov E.B., Drobakha G.A., Bilchuk V.M., Tristan A.V., 2008)*:

- improvement of automated systems of command and control of troops and weapons (clearly showing changes in the transition to the development and creation of automatic weapons control systems);

- improvement of high-precision weapons, which, due to their entry into the information environment of the "combat space", can receive certain adjustments even after launch;

- improvement of intelligence means, with certain changes in the expansion of their use, along with the transformation of unmanned intelligence means into traditional ones, various detectors and sensors that can operate autonomously for a long time and be at sufficiently long distances;

- improvement of artificial intelligence-controlled weapons and robotic warfare systems.

The US Department of Defense believes that in order to achieve victory in armed conflicts, it is necessary to receive, transmit and process information as close as possible to real time *(Bochkovyi, O.V., 2010)*. Victory over the opponent is ensured by an informational advantage. It allows you to adequately understand the current situation on the battlefield, to make timely decisions that will anticipate the actions of the enemy. For this purpose, the development and use of intelligent weapons and robotic means are provided for in the framework of the system of increasing combat capability and mobility in the US forces. The system of combat support of the troops under the new concept additionally includes: a system of operational replanning of the operation, which reduces time consumption tenfold, a subsystem of operational mapping, technologies for training soldiers to act in non-standard conditions, etc. Substantial reforming of the procedures for operational and full implementation of tasks in the field of defense is being carried out in Ukraine as well. The latest technologies for automation of defense planning processes and corresponding software and technical tools have already been developed on a scientific basis. At the same time, among the number of information-analytical and software systems implemented in the Armed Forces of Ukraine, IAS "Resurs" can be singled out as the basic one, which made it possible to comprehensively solve information and calculation tasks, modeling tasks, as well as provide timely information on the basis of a system approach. objective and sufficient information and means of comprehensive analysis to decision-makers, from the unit commander to senior management. In addition, under the state order, the Scientific Research Institute of Automated Computer Systems "Ekotech" is developing a whole complex of information and analytical systems ("IAS of Defense Planning Support of the Armed

Forces of Ukraine", "IAS of Automated Accounting of Armed Forces Personnel" and others), which are already undergoing inspection and will soon be implemented in the practical activities of the Armed Forces of Ukraine *(Bochkovyi, O.V., 2010).*

The use in the work of military management bodies of standardized procedures of planning stages as a form of military decision-making by the commander and headquarters of the unit according to NATO standards leads to a number of problematic issues, the solution of which is possible in the case of implementation in the military decision-making process (MDMP - Military Decision- Making Process) of information and analytical technologies that combine methods of collecting and processing information during the summarization of conclusions from the analysis of the task and assessment of the situation, specific methods of their diagnosis, analysis of options and synthesis of the method of action of subordinate forces and means, as well as assessment of the possibilities of achieving the final the purpose of performing a service-combat task *(Kolomiitsev, O. V., Obriadin, V. V., Horielyshev, S. A., 2023).*

Since 2018, separate information systems of various levels have been used: Delta, "Kropyva", "Virazh-planshet", GisArta, etc. (Table 1). All the listed systems work at the tactical level *(Horielyshev, S. A., Ivanchenko, A. O., Bashkatov. Ye. H., 2023).*The special software complex "Viraj-tablet" is an automated geographic information system (GIS) for collecting, processing, displaying and analyzing information about the air situation, which is created by the radio engineering troops of the Air Force of the Armed Forces of Ukraine in order to automate the procedures for controlling, storing and issuing information about the air situation. The GisArta information system is an automated system for managing artillery units, which takes into account the specifics of planning and conducting combat operations of these units and the requirements for obtaining actual data on the results of combat operations. The "Kropyva" software complex (PC) is a GIS-based tactical link management system for creating intelligent maps in combination with devices and instruments, for planning, calculations and orientation on the terrain. Today, this PC is used by various units of the ground forces of the Armed Forces, the National Guard of Ukraine, and the Territorial Defense (artillery, armored vehicles, infantry and reconnaissance units) *(Horielyshev, S. A., Ivanchenko, A. O., Bashkatov. Ye. H., 2023).*

In contrast to the military industry, there were no fundamentally new, technologically revolutionary methods of information support for law enforcement activities, which had a negative impact on the state of crime, the protection of the rights, freedoms, and life values of citizens. The criminogenic situation that has developed in Ukraine reflects the tendency to increase the number of appeals from citizens about criminal events. Accordingly, the burden on the employees of the operational divisions of the Ukrainian Armed Forces increases, which, combined with the staffing

problems accumulated in recent years, only complicates the crisis of the law enforcement system. Therefore, it is necessary to create a single national information system for law enforcement agencies. The introduction of a unified state-wide information system will not only significantly reduce the workload of operatives, but will also allow the effective and efficient use of state information resources in real time.

Table 1 - List of combat information systems.

Name	Purpose	Year
«Ukrop» (MyGun)	Calculation for artillery fire, offline map, orientation	2009
GisArta	Orientation, planning, calculation for artillery	2014
«Kropyva»	Calculation for artillery fire, planning, plotting the tactical situation, unit management, reconnaissance, orienteering	2014
«Topo» (Topic)	Orientation, drawing a tactical situation	2014
«Bronia»	Calculation for shooting from grenade launchers, mortars, tanks, orientation	2015
«Terminal»	Tactical situation, orientation	2015
ComBat Vision	Intelligence, orientation, decision support	2015
Delta	Orientation, tactical situation, unit management	2016
«Dzvin-AC»	Command and control of combat operations at the command level	2016
«Virazh- tablet»	Collection, display and analysis of information about the air situation	2016
MilChat	Exchange of messages, tactical situation, broadcasting of geolocation	2018
«Prostir»	Forces and weapons command at the brigade level	2021

However, the effective application of the concept of information advantage in ORD is impossible without an effective and efficient information model, which currently depends entirely on the management system in internal affairs bodies. That is, the information model repeats the hierarchy of management bodies and all system solutions take this into account as a given.

Security forces need different types of IATs during the implementation of the assigned tasks. Thus, for the National Police of Ukraine (NPU), priority is the use of databases (DBs), which store information about offenders, criminal events, etc. Both the NPU and the State Border Service of Ukraine (SBSU) need recognition systems for wanted objects (offenders). Such national databases can be used by other subjects of the security forces during the implementation of the assigned tasks, which are inherent only to these subjects. Automated control systems (ACS) are needed by all security forces without exception. Not only in matters of interaction and data exchange, but also in matters of general leadership, management of units (groups) and weapons at the state level. According to Table 1, security forces performing combat missions require decision support systems (DSS), geographic information systems (GIS). The needs of the security forces in information and analytical technologies are shown in Table 2.

Table 2 - Needs of security forces in information and analytical technologies

№	Subject of the security forces	IAT					
		DB	ACS	Document management systems	Disp. images	DSS	GIS
1	NGU (MIA)	-	+	+	-	+	+
2	NPU (MIA)	+	+	+	+	-	-
3	State Emergency Service (MIA)	-	+	+	-	-	+
4	Security Services of Ukraine	+	+	+	+	+	+
5	State Border Service	+	+	+	+	+	+

The information and analytical support of the security forces of Ukraine has specific decision support systems, simulation models of service and combat operations, databases and recognition systems for wanted objects. General information technologies of the security forces as a subject of state security are ACS and document management systems.

To date, there is a need for the formation of requirements for the national information system of the security forces, and in the future it will be created. Modern challenges faced by our state require immediate improvement of the state administration system. One of the ways to improve the state management system is the creation of a state-wide information system for the management of security forces.

Conclusions. The development of information and analytical support of the security forces of Ukraine is closely related to the development of technologies, fundamental branches of science (mathematics, physics, chemistry). The increase in the productivity of computer technology allows us to move to the use of artificial intelligence in decision support systems. Today, management bodies widely use information technologies during decision-making. Factors affecting the information and analytical support of the security forces, obtained using the Ishikawa diagram, allow determining the impact on state security during the performance of service and combat tasks.

It is expedient to develop the IAS in the following directions: the introduction of the latest information technologies for decision-making during the performance of official and combat tasks; creation of new technical solutions during the development (modernization) of IAS; development and improvement of the information infrastructure of the security forces taking into account national and international standards; creation of IAS taking into account the requirements for ensuring interaction between existing and created information systems in the security forces; use of flexible technological platforms during the implementation of the developed IAS; taking into account the requirements for fault tolerance and disaster resistance of IAS, which are being developed; implementation of automatic identification and authentication of IAS users, regulated access and data exchange,

ensuring the necessary level of information protection against external and internal threats; improvement of the organizational structure of the IAS, which is being developed.

Modern challenges faced by our state require immediate improvement of the system of information and analytical support of the security forces of Ukraine.

References:

Taylor James G. Support of JCATS Limited Verification and Validation: report / James G. Taylor, Beny Neta. – Monterey, California: Naval postgraduate school, September 2001. – 51 p.

Bogush, V. M., Krivutsa, V. G., Kudin, A. M. (2004). *Informatsiina bezpeka: Terminolohichnyi navchalnyi dovidnyk [Information security: Terminological educational handbook]*. Kyiv: OOO «D.V.K.» [in Ukrainian].

Bochkovyi, O.V. (2010). Zastosuvannia informatsiino-analitychnykh tekhnolohii v operatyvno-rozshukovii diialnosti [The use of information and analytical technologies in operational and investigative activities]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav imeni E.O. Didorenka – Bulletin of the Luhansk State University of Internal Affairs named after E.O. Didorenko, 4,* 272-279 [in Ukrainian].

Horielyshev, S. A., Ivanchenko, A. O., Bashkatov. Ye. H.. (2023). Prohramnyi kompleks «Kropyva» yak element perspektyvnoi avtomatyzovanoi systemy upravlinnia Natsionalnoi hvardii Ukrainy [The "Kropyva" software complex as an element of the promising automated control system of the National Guard of Ukraine]. *Chest i zakon – Honor and law, 4(87),* 22-29 [in Ukrainian].

Matsko O. Y., Mykus S. A., Solonnikov V. H. (2021). *Zastosuvannia suchasnykh informatsiinykh tekhnolohii u naukovii diialnosti [Application of modern information technologies in scientific activity]*. Kyiv: NUOU im. I. Cherniakhovskoho [in Ukrainian].

Kolomiitsev, O. V., Obriadin, V. V., Horielyshev, S. A. (2023). Informatsiino-analitychni tekhnolohii zabezpechennia pryiniattia viiskovoho rishennia za standartamy NATO pid chas vykonannia zavdan u sferi derzhavnoi bezpeky [Information and analytical technologies to ensure military decision-making according to NATO standards when performing tasks in the field of state security]. *Bezpeka Derzhavy – State security, 1(1),* 27-39 [in Ukrainian].

Kormych, B. A. (2008). *Informatsiina bezpeka: orhanizatsiino-pravovi osnovy [Information Security: Organizational and Legal Foundations]*. Kyiv: Condor [in Ukrainian].

Gorodnov, V.P., Drobakha, G.A., Yermoshin, M.O., Smirnov, E.B., Tkachenko, V.I. (2004). *Modeliuvannia boiovykh dii viisk (syl) protypovitrianoi oborony ta informatsiine zabezpechennia protsesiv upravlinnia nymy (teoriia, praktyka, istoriia rozvytku) [Modeling of combat operations of air defense troops (forces) and information support of their management processes (theory, practice, history of development)]*. Kharkiv: KhVU [in Ukrainian].

Nosach A.V. (2019). Zahrozy natsionalnii bezpetsi yak oboviazkova oznaka zlochynnosti, shcho posiahaie na derzhavnyi suverenitet i terytorialnu tsilisnist Ukrainy [Threats to national security as an obligatory sign of crime encroaching on the state sovereignty and territorial integrity of Ukraine]. *Pravo i suspilstvo – Law and society, 3,* 50-56 [in Ukrainian].

Tkachenko V.I., Smirnov E.B., Drobakha G.A., Bilchuk V.M., & Tristan A.V. (2008). *Teoriia pryiniattia rishen orhanamy viiskovoho upravlinnia [The theory of decision-making by military administration bodies]*. Kharkiv: KhVU [in Ukrainian].

Tkachuk, P.P., Gula, R.V., Sivak, O.I., Shchurko, O.M., & Shemchuk, V.V. (2015). *Informatsiina viina i natsionalna bezpeka [Information war and national security]*. L.: NASV [in Ukrainian].

Shemchuk V. (2020). Zahrozy informatsiinii bezpetsi: problemy, vyznachennia ta podolannia [Threats to information security: problems of definition and overcoming]. *Paradyhmy yurydychnykh nauk i derzhavnoho upravlinnia – Paradigms of legal sciences and public administration, 1(7),* 285-296, https://doi.org/10.32689/2617-9660-2020-1(7)-285-296 [in Ukrainian].

DOI 10.5281/zenodo.10821969
UDC 355.6:658.7:351.74/.76

CHAPTER 14.
SECURITY FORCES OF UKRAINE POTENTIAL JUSTIFICATION IN CRISIS SITUATIONS RESPONSE

Vladyslav YEMANOV
Doctor of scienes in public administration, senior research
National Academy of the National Guard of Ukraine,
(3, Maidan Zahisnykyv Ukrainy, Kharkiv, 61001, Ukraine)
mail@nangu.edu.ua
https://orcid.org/0000-0001-5055-8852

Abstract. The role and place of security forces of Ukraine in responding to crisis situations have been studied. The genesis of security forces of Ukraine actions during crises in the paradigm of state security has been characterized. Regulatory legal acts in the field of ensuring national security have been considered, and the definition of a "crisis situation" has been examined. It has been determined that in the system of ensuring national security, the main subjects of ensuring state security are security forces. An assessment of the level of military security of the country based on the level of the military-economic potential of the state, which is the basis of protecting its national interests, has been carried out. It has been established that the military potential depends on the degree of saturation with weapons, military and special equipment of security and defense forces. The speed of production and restoration of weapons, military and special equipment will be the main feature of the military potential of the state. One of the requirements for security forces is the requirement of balance, which is expressed in establishing rational proportions among different types of weapons. In each country, these proportions are established taking into account the features of the military doctrine, the specificity of the tasks assigned to the Armed Forces, the levels of development of technology, historical traditions, and other factors.

Keywords: national security, technical support, security forces, security and defense sector of Ukraine, assigned tasks, security ensurance, crisis situations.

Introduction. One of the main tasks of the state policy in the defense area of the sovereignty and territorial integrity of Ukraine is to maintain the security and defense components in a combat-ready condition, in particular by organizing the appropriate technical support. Resisting the armed aggression of the russian federation against Ukraine depends on the effective use of all weapons and

special equipment types, which make up the material and technical basis of the military capability of the security and defense forces. A characteristic feature of conducting modern military operations is the massive use of technical means to conduct security operations. The experience of technical support implementation in the conditions of the security forces of Ukraine working to crises indicates several problematic support issues that need to be solved, as they significantly affect the quality of the performance of assigned tasks.

The development and improvement tasks of the security forces of Ukraine are defined by the national security strategies of Ukraine (approved by the Decree of the President of Ukraine dated 14.09.2020 No. 392/2020), ensuring state security (approved by the Decree of the President of Ukraine dated 16.02.2022 No. 56/ 2022), military security of Ukraine (approved by the Decree of the President of Ukraine dated 25.03.2021 No. 121/2021), the order of the Ukraine's Cabinet of Ministers dated 14.06.2017 No. 398-r "On approval of main development directions of weapons and military equipment for a long-term period".

The Ukrainian security forces are equipped with a variety of new foreign-made equipment, while national equipment is 60% morally and physically outdated, has been in operation for more than 25 years, and needs updating (modernization). The intensive development of means and methods of performing tasks in crises by Ukraine's security forces places increased demands on the recovery system, in particular, on moving means of repairing equipment. However, there are also unanswered problems in this direction, because the available moving means of repairing equipment in the security forces units of Ukraine do not allow covering the entire necessary repair fund of equipment. It is linked with the excessive consumption of motor resources, partial inconsistency and imperfection of the diagnostic and technological equipment of the available forces and means of evacuation and repair, the inconsistency of property stocks to the provision of the vehicles, the increase in the range of material resources, and the mismatch of the organizational and staffing structure of technical support.

Therefore, the system of providing security forces of Ukraine needs further development, and in some directions, reformation. Based on the scientific and methodical bases, it should be noted that the technical support of the Ukrainian security forces as a system is a combination of equipment, units' personnel who use such equipment, units' personnel who evacuate and repair damaged vehicles, provide management of technical support, and management units which carry out state orders, procurement and supply of special equipment and weapons. According to these conditions, the research's relevance of the chosen topic is determined by the necessity to ensure the appropriate level of technical support for the Ukrainian security forces in crises through the formation and development of state management mechanisms of the technical support system of the Ukrainian

security forces.

The role and place of Ukrainian security forces in responding to crises. Today's issues of Ukraine have a significant impact on national security. The Ukrainian security forces perform tasks aimed at supporting national security during crises. It is the improvement of state management mechanisms in the field of ensuring Ukrainian national security will allow an increase in the effectiveness of the actions of the security forces.

According to the definition by Sytnyk H.P. "State administration is an organized process of leadership, supervision and control of states agencies to ensure the development of society, responding to actual threats, as well as preventing crisis phenomena" *(Sytnik G., 2012)*. This process is implemented through state policy as a program of actions or a system of targeted measures. State policy in the field of ensuring national security is the measures' system of purposeful activity for subjects of this policy at a specific stage of the state's development, which is developed and implemented based on defined principles. Most specialists use the term "the state policy of national security " as actions, measures, institutions of state authorities, that ensure the preservation of the integrity of society, social progress, in the context of maintaining a mutually accepted balance of individual (citizen) interests, society and the state *(Sytnik G., 2012)*. Thus, ensuring national security can be attributed to the competence of the social and political sphere.

The law of Ukraine dated June 21, 2018 No. 2469-VIII "On the National Security of Ukraine" defines in Article 3 that state policy in the spheres of national security and defense is aimed at protecting: the lives and dignity, constitutional rights and freedoms, safe living conditions of an individual and citizen; society's democratic values, well-being and conditions for sustainable development; state's constitutional system, sovereignty, territorial integrity and inviolability; and to protect the territory and the natural environment from emergencies.

State management in the field of national security is considered the influence of state authorities on ensuring to saving of an individual or citizen's life, the temporary development of social relations in society, the protection of the constitutional order, sovereignty, territorial integrity, and inviolability of the state, prevention and/or minimization of the consequences of crisis and emergencies in the social, political, economic, man-made and natural situations; a system of legal, organizational, and control measures of the state to respond to actual threats using various means and forms, methods.

Decree of the President of Ukraine dated January 12, 2015 No. 5/2015 "Sustainable Development Strategy "Ukraine – 2020" was the basis for reforming state policy in the field of ensuring Ukraine's national security. This document demonstrates the "security vector" as one of the main vectors of the movement regarding the introduction of European standards of Ukrainian living

and Ukraine move to the fore in the world. One of the main measures of implementing the reform of the national security and defense system is the optimization of the logistics support system.

The legal basis of state policy in the spheres of national security is the Constitution of Ukraine, relevant laws of Ukraine, international treaties, the binding consent of which has been given by the Verkhovna Rada of Ukraine, and other normative legal acts issued to implement the Constitution and laws of Ukraine. Among such documents, which declare the issue of ensuring the national security of Ukraine, the following should be noted:

– Law of Ukraine "On National Security of Ukraine";

– National Security Strategy of Ukraine *(Reznikova O., 2022)*;

– Military doctrine of Ukraine;

– Concept of the development of the security and defense sector of Ukraine;

- Strategic Defense Bulletin of Ukraine.

Article 1 of the Law of Ukraine "On the National Security of Ukraine" defines the term "national security" as "the protection of state sovereignty, territorial integrity, democratic constitutional order and other national interests of Ukraine from real and potential threats". National security threats are defined phenomena, trends, and factors that be/or can be reasons for difficulties or impossibility of the realization of national interests and the preservation of national values of Ukraine.

National interests are the vital interests of an individual, society and the state, the implementation of which ensures the state sovereignty of Ukraine, the progressive democratic development, and safe living conditions and the well-being of the citizens.

Analyzing the Law of Ukraine, we can conclude that the objects of national security are:

– an individual and a citizen (their life and dignity, constitutional rights and freedoms, safe living conditions);

– society (its democratic values, well-being and conditions for sustainable development);

– the state (its constitutional system, sovereignty, territorial integrity and inviolability);

– the territory of the country and the surrounding natural environment.

The subject of ensuring national security is the security and defense sector of Ukraine as the system of state authorities, the Armed Forces of Ukraine, other military formations which were formed by the laws of Ukraine, law enforcement and intelligence agencies, state agencies of special purpose with law enforcement functions, civil defense forces, defense industrial complex of Ukraine. Security forces are law enforcement and intelligence agencies, special state agencies with law enforcement functions, civil defense forces, and other agencies assigned by the Constitution and laws of Ukraine functions to ensure the national security of Ukraine, which are different from the defense

forces. That is, the main such subjects are state authorities at all levels of management, security forces, and defense forces, as well as citizens of Ukraine and associations of citizens.

The definition "state security" can be found as "a state security is the protection of state sovereignty, territorial integrity and the democratic constitutional order and other vital national interests from real and potential threats of a non-military nature".

The Decree of the President of Ukraine dated May 26, 2015 No. 287/2015 "National Security Strategy of Ukraine" identifies current threats to the national security of Ukraine. Accordingly, in the context of ensuring state security, non-military threats include:

– ineffectiveness of the system of ensuring national security and defense of Ukraine, insufficient resource provision and inefficient use of resources in the security and defense sector;

– corruption and inefficient system of public administration;

– economic crisis, exhaustion of the state's financial resources, decrease in the standard of living of the population; the absence of clearly defined strategic goals, priority areas and tasks of social, economic, military, scientific, and technical development of Ukraine, and effective mechanisms for the concentration of resources to achieve such purposes *(Horbulin V., Kachynskyi B., 2007).*

It needs to consider the normative legal acts in the field of ensuring national (state) security and examine the definition of "crisis situation" *(Belay S.V., Bondarenko O., 2017).* In our days, there is no such definition of "a crisis situation" in the legislation that would fully and comprehensively characterize this concept. The Code of Civil Protection of Ukraine operates with the concept of "emergency situation" and interprets it as "an emergency situation is a situation on a separate territory or a subject of commercial activity on the area or a water object, which is characterized by a violation of the normal conditions of human life, caused by a catastrophe, accident, fire, a natural disaster, an epidemic, an epizootic, an epiphytotic, the use of pesticides or another dangerous event that has led (may lead) to a threat to the life or health of the population, a large number of dead and injured people, causing significant material damage, to the impossibility of living population on such a territory or object, introduction of a subject of commercial activity on the area" *(Belay S.V., Bondarenko O., 2017)*. Unfortunately, the specified definition does not establish a connection with the category "crisis situation", although this concept is increasingly used in normative legal acts related to ensuring the national security of Ukraine.

Thus, the National Security Strategy of Ukraine *(Reznikova O., 2022)* among the main measures to create an effective security and defense sector (subsection 4.2) defines "... centralized management of the security and defense sector in peacetime, in crisis situations as a threat of the national security, and in a special period, interdepartmental coordination and interaction". One of the

main tasks of increasing the defense capability of the state (subsection 4.3) is "... preparing the state to repel armed aggression, increasing the ability of state authorities, military administration and local self-government agencies, defense forces, the civil defense system, the defence industry complex to function in crisis conditions situations that is a reason of threat of the national security and a special period". Among the measures of the special partnership with NATO (subsection 4.7) is defined "... creation of an effective mechanism for responding to crisis situations that threaten national security" *(Reznikova O., 2022).*

The implementation of the Concept of the development of the Ukrainian security and defense sector will be achieved by "... combining the operational capabilities of the components of the security and defense sector to ensure a timely and adequate response to crisis situations that threaten national security". To achieve the purpose of the Concept, it is planned to implement a task complex, which consists of "...the forces and means of the security and defense sector got the defined basic operational (combat, special) capabilities necessary for a guaranteed response to crises that threaten national security".

Also, subsection 3.4 states that "...the main purpose of the development of the National Guard of Ukraine is the creation of new units as a part of the National Guard of Ukraine, which can interact with other components of the security and defense sector, can perform a wide range of law enforcement tasks and effectively respond to crises that threaten national security".

In Chapter 3 of the Strategic Defense Bulletin of Ukraine, the mechanism for implementing the defense reform is specified, favorable and negative factors are identified, one of the favorable factors is "...studying and implementing the experience of the functioning of military management agencies and the performance of tasks by troops (forces) during a response to crises".

Thus, analyzing these normative legal documents, it is possible to note that a new term "crisis situations threatening the national security of Ukraine" has been introduced, which characterizes the situation on the eve of the introduction of a special period. The term "crisis situation" was enshrined at the legislative level by the Law of Ukraine dated 25.12.2014 No. 43-VIII "On Amendments to the Law of Ukraine "On the National Security and Defense Council of Ukraine" regarding the improvement of coordination and control in the field of national security and defense", which states that "...a crisis situation is considered to be an extreme aggravation of contradictions, acute destabilization of the situation in any sphere of activity, region, country".

Yu. P. Babkov and M. M. Adamchuk in their work *(Babkov Yu., AdamchukM., 2016)* have provided their own author's definition of the concept of "crisis situation". "A crisis situation is a situation with a high level of tension that has developed or can develop as a result of actions that can lead to damage to the vital interests of a person and a citizen, characterized by an extreme aggravation

of contradictions, acute destabilization of the situation in any sphere of activity, region, country, the response to which requires the involvement of additional forces and means of state authorities, local self-government agencies, security forces, defense forces and another military, law enforcement formations and civil defense forces formed by the Laws of Ukraine, public organizations and citizen associations, within a limited period, enterprises, institutions and organizations without the introduction of extraordinary administrative and legal regimes" *(Babkov Yu., AdamchukM., 2016).*

These authors separate crises from extraordinary administrative and legal regimes. That is, we believe that such a definition is correct for a crisis situation that threatens state security. Also, based on the analysis of the listed normative legal acts, it is possible to note that a gradation has been introduced for three periods of functioning of the security and defense sector:

- peaceful time or everyday activities;
- crisis situations during peacetime;
- a special period (wartime) *(Horbulin V., Kachynskyi B., 2007).*

In our opinion, it is necessary to consider the classification by crisis nature that threatens state security in more detail. Crises of a military-political nature, at first, should be classified, by the provisions of the Law of Ukraine "On National Security of Ukraine", as crisis situations that threaten military security. After all, the specified Law defines military security as the protection of state sovereignty, territorial integrity and the democratic constitutional order and other vital national interests from military threats *(Horbulin V., Kachynskyi B., 2007).*

However, in our opinion, before the introduction of a special period (wartime), the security forces will be involved in responding to the specified crisis situations, namely, intelligence agencies, special state agencies and military formations with law enforcement functions and others *(Horbulin V., Kachynskyi B., 2007).*

It should be noted that in a special period (wartime) the main subjects of response to crisis situations of a military and political nature should be the defense forces headed by the General Staff of the Armed Forces of Ukraine, namely the Armed Forces of Ukraine, as well as others formed under the laws Ukraine's military formations, law enforcement and intelligence agencies, special purpose agencies with law enforcement functions, which are entrusted with the functions of ensuring the defense of the state by the Constitution and laws of Ukraine.

Therefore, the Armed Forces are not part of the security forces, which rely on the main efforts in responding to crisis situations in peacetime, but most of the security forces in wartime are part of the defense forces. Thus, peacetime military-political crisis situations refer to crisis situations that threaten state security.

Crisis situations of a criminogenic, socio-political and socio-economic, man-made and natural

character are undoubtedly crisis situations that threaten state security. In addition, the specified situations are related to the internal security system and its subsystems of public security and civil protection, which will be discussed below. It should be noted that the specified crisis situations correspond to all threats to the national security of Ukraine of a non-military nature, defined in the National Security Strategy of Ukraine *(Horbulin V., Kachynskyi B., 2007)*.

Thus, the issue of response to crisis situations remains relevant and requires the development of appropriate state management mechanisms for the actions of state security forces. One of the key features of peacetime crises is their arising at any time in any field of activity and in any region, which undoubtedly leads to damage to the vital interests of citizens and their associations, objects of social infrastructure, enterprises, state authorities, etc.; they require the involvement of additional forces and means of state authorities, local self-government agencies, and security forces of various departments within a limited period; as a rule, they don't require the introduction of extraordinary administrative and legal regimes.

Currently, it is important to establish the role and place of state security in the system of ensuring national security under these conditions. It should be noted that there is no concept of "a system of ensuring national security" in the current legal documents. Bielai S.V. considers that "the system of ensuring national security is a subject complex organized by the state, that is to say, state authorities, local self-government agencies, public organizations, individual citizens and their associations, which are in relations and connections with each other, forming a defined integrity, unity, united by goals and objectives to protect Ukrainian national interests, effective functioning of the system of ensuring national security of Ukraine itself, and carry out coordinated activities within the framework of Ukrainian legislation" *(Belay S., 2015)*.

Thus, it is possible to determine the structural scheme of the national security system.

The security forces are the main subjects of ensuring state security in the system of ensuring national security. The Law of Ukraine "On National Security of Ukraine" defines and delimits the powers of state agencies in the spheres of national security and defense, creates a basis for the integration of policies and procedures of state authorities, other state agencies whose functions relate to national security and defense, security forces and defense forces, the system of command, control and coordination of operations of security forces, and defense forces is defined. This law provides the definition of security forces "Security forces are the law enforcement and intelligence agencies, state agencies of special purpose with law enforcement functions, civil defense forces and other agencies that are entrusted with the functions of ensuring the national security of Ukraine by the Constitution and laws of Ukraine". Accordingly, the main forces involved in actions during most peacetime crisis situations that threaten state security are the Security Service of Ukraine and security

forces led by the Ministry of Internal Affairs of Ukraine (National Police of Ukraine, National Guard of Ukraine, State Emergency Service, State Border Service of Ukraine).

The specified subjects of the state security system are in relations and connections with each other and respond to crisis situations that can threaten the state security of Ukraine. That is why it is necessary to investigate the mechanisms of state management of the actions of security forces when responding to crisis situations that can threaten state security.

The main role is management mechanisms, which, in our opinion, are a certain lever in the state system in the state policy of responding to crisis situations that threaten state security.

A significant number of options for defining the concept of "control mechanisms" have been provided by native and foreign scientists. According to the definition in the technical field, a mechanism (Greek: μηχανή mechané - machine) means the internal structure of a machine, device, or apparatus, which helps them to start working and is intended for the transmission of motion and energy conversion. That is, the direct influence of the subject of management on the object of management to obtain the desired result, for example, to ensure the movement of the object is the main stage of the management process. Based on the fact that the transfer of movement and energy transformation characterize the relationship between the subject and the object of management, the use of the concept of mechanism from the standpoint of technology satisfies the conditions of management in general and state management in particular.

In management theory, mechanisms are understood as the using of certain means with the help of selected methods to solve established problems *(Bondar O., 2012)*. In our opinion, this approach is appropriate for the theory of public administration, because a whole complex of practical management tools and methods is used to solve certain public administration problems. Scientists who study economics can use the concept of "management mechanisms" as the understanding of a complex system that makes it possible to transform the material and spiritual needs of people into means of production through labor activities and satisfy consumer demand. The basis of this mechanism, following economic principles, is a system of incentives, which is divided into two subsystems: command and administrative incentives that compel work, and social and economic ones that interest employees in highly efficient work.

Anti-crisis managers provide a more detailed definition of management mechanisms in the conditions of the occurrence of crisis phenomena. The main task of anti-crisis management is to determine the role and place of the anti-crisis mechanism in the social and economic system of society. Thus, the mechanisms of state management in the field of crisis management are a complex of influence means to obtain the planned result in terms of minimizing the consequences of such phenomena and restoring the sustainable development of society as soon as possible. This aggregate

holds certain components that carry out the work of the management mechanism, which is an element of the social and economic system of the state.

In his work Bielai S.V. *(Bielai S., 2015)* studied the concept of "mechanism of public administration", and analyzed such definitions by the authors given above, he established that in the science of public administration, there are two main approaches to defining the concept of the mechanism of public administration, thus the understanding of the concept in a narrow and wide sense. For example, N. R. Nyzhnyk and O. A. Mashkova interpret the mechanisms of state management in a narrow sense as "... a part of the management system that provides influence on the factors on the condition of which the result of the activity of the management object depends" *(Mashkov O. , Nizhnik N., 1998)*. The most acceptable definition of the concept of "mechanism of public administration" in the broad sense is the definition of scientists V. M. Knyazev and V. D. Bakumenka, namely "...practical measures, means, levers, incentives, with the help of which state authorities influence on society, production, any social system to achieve the goal complex" *(Didivska L., Golovko L., 2007).*

So, the narrow interpretation of the state management mechanism is a complex of certain parts designed to implement management decisions; a wide interpretation of the state administration mechanism is a complex system of state agencies organized to perform state administration tasks.

Under the mechanisms of state management of response to crisis situations that threaten state security, it is appropriate to understand a set of special practical measures, means, levers, and incentives, with the help of which security forces influence the system of ensuring national security to reduce the level of threats to state security.

Practice shows that when crisis situations arise, there is a need to switch to centralized management of all forces (security forces, state and local self-government agencies, public organizations and citizen associations) involved in responding to such situations, which indicates the need for state influence. During crisis situations, significant threats to state security arise. Ensuring internal security as a component of state security is the most significant function of the state and is expressed in ensuring the stability of state and non-state institutions, social and legal norms in the state, and the lives of citizens. One of the main tasks of internal security entrusted to public authorities and security forces, among other things, is the task of protecting public order, implementing public security measures, and ensuring civil protection within the limits of their powers. To resolve crisis situations by threatening state security, the following mechanisms of state administration are mainly used organizational (and structural, economic, administrative, etc.); legal (based on organizational and managerial and administrative and executive activities exist); financial and economic; motivational; complex; etc. The basis of mechanisms for responding to crisis situations that threaten

state security is the internal security system, which includes public security and civil defense subsystems.

The internal security system is not enough studied. According to the accepted definition, ensuring internal security is the most important task of the state and is revealed in ensuring the functioning of state and non-state institutions, social and legal norms in society, sustainable development, life activities of citizens, etc.

Ponomarenko H. O. *(Ponomarenko H., 2007)* defines the internal security of the state "...in wide and narrow meanings. In a wide sense, it means protection from all possible types of internal threats, in a narrow sense, only from those that are the result of committing crimes... Ensuring the internal security of the state is understood as a necessary condition for the person's life, society, and the state, a system of legal, organizational, personnel, informational, and other measures implemented by specially authorized entities to protect people, society and the state from internal threats that are a consequence of committing crimes". Yu. V. Nikitin shows internal security as a general category that is part of the category "national security". In his opinion, internal security reveals the state of life of people in society and the corresponding threats to this process. Internal security is dependent on state and public institutions, their development and mutual relations. The main task of internal security is "... to protect the rights and freedoms of all sections of the population using democratic and legal methods, to counter anti-social and anti-democratic manifestations, no matter who they come from, even from the state". Nikitenko defines the internal security of the country as the protection of the vital interests, society and the state from internal threats, which is a necessary condition for the preservation and multiplication of spiritual and material values. It is worth agreeing with the definitions of internal security given above while noting that gradation into a broad and narrow understanding of the security sphere is appropriate.

Therefore, internal security in a wide sense is a state of protection of the vital interests, society, and the state from internal threats, and in a narrow sense, it is a state of protection of the vital interests, society, and the state from threats that are a consequence of committing offenses.

The system of ensuring internal security, according to the definition in a wide sense, includes state and local self-government agencies that, within the limits of their competence, provide activities to ensure internal security, in a narrow sense, it is state security forces.

Public safety is a component of the state's internal security. Ensuring public safety is a complex of measures implemented by state authorities and local self-government agencies to avert threats to the person and society. Scientific sources state that the public security system represents "... a complex of state authorities, agencies and services, state and non-state organizations, individual citizens who, within the limits of their competence or personal initiative... providing activities to

ensure public security". However, A.V. Bassov explained this concept as a wide concept that includes the following elements, for example, the content of public security, the system of public security entities, the tasks of public security entities and principles of activity, a list of threats, that pose a danger to public safety, means of ensuring civil safety.

Bassov A.V. *(Basov A., 2010)* notes that public security should be understood as "...a system of social relations regulated by legal norms, which ensures personal safety, public peace, favorable conditions for work and recreation of citizens, normal functioning of state agencies, public associations, enterprises, institutions and organizations from the threat of criminal and other illegal acts, violation of the procedure for using sources of increased danger, objects and substances removed from free civilian circulation, negative man-made and natural phenomena, and special circumstances". In our opinion, this definition is thorough and acceptable.

One of the components of the subsystem of the internal system is the civil protection system, and its forces are responsible for a reaction to a sufficiently large, layer of crises that threaten the state security of Ukraine. The Civil Protection Code of Ukraine, enacted by the Law of Ukraine dated October 2, 2012 No. 5403-VI, defines "civil protection as a state function aimed at protecting the population, territories, natural environment and property from emergencies by preventing such situations, liquidating their consequences and providing assistance to victims in peacetime and in a special period". It is also stated that the liquidation of the consequences of an emergency includes emergency rescue and other urgent works, which are in the event of an emergency situation and are aimed at stopping the action of dangerous factors, saving lives and preserving the people's health, and at the localization of the emergency situation zone. In his scientific article that "prevention and elimination of the consequences of man-made and natural emergencies, preservation of population lives and health, ensuring sustainable development of the country is one of the components of the national security of the state". "Mechanism of emergency state management" should be interpreted as a complex of methods, methods and means of the regulatory influence of the state, which are used by it to prevent and reduce the negative effects of emergencies, and further scientific research should be focused on the development of theoretical provisions and practical recommendations, aimed at prevention of emergencies and proper response in case of their occurrence. System of support for decision-making by state administration agencies in emergency situations (incidents) through the use of situational centers will improve the quality of such decisions, increase the effectiveness of combating emergency situations (incidents) in Ukraine, as evidenced by the foreign experience of using such structures.

Thus, we are forming a system of responding state management to crises that threaten state security. At the national level, the President, the Verkhovna Rada, and the Cabinet of Ministers of

Ukraine provide organizational and rulemaking activities to ensure the state security of Ukraine. The main advisory and coordinating agency is the National Security and Defense Council of Ukraine. Ministries and other central agencies of executive power, including subordinated central agencies of security forces, are the main executors of measures to ensure state security at the national level. At the regional and local levels, local public administration agencies (executive authorities and local self-government agencies) and regional units of security forces respond to crisis situations that threaten state security.

It is appropriate to dwell separately on the tasks of certain formations of the security forces in the context of their involvement in responding to crisis situations that threaten state security. The main forces from the security forces involved in responding to the vast majority of crisis situations are undoubtedly the units of the Security Service of Ukraine and formations subordinate to the Ministry of Internal Affairs, namely the National Police of Ukraine, the National Guard of Ukraine, the State Border Service of Ukraine, the State Service of Ukraine on emergency situations *(Horbulin V., Kachynskyi B., 2007)*.

According to the Law of Ukraine dated March 25, 1992 No. 2229-XII (in the version dated August 2, 2018) the Security Service of Ukraine is a special state agency with law enforcement functions that ensures the state security of Ukraine. The Security Service of Ukraine is entrusted with the protection of state sovereignty, constitutional order, territorial integrity, economic, scientific and technical and defense potential of Ukraine, the legitimate interests of the state and the rights of citizens against the intelligence and subversive activities of foreign special services, encroachments by individual organizations, within the limits of competence defined by the law, groups and individuals, and ensuring the protection of state secrets. The tasks of the Security Service of Ukraine also include the prevention, detection, termination and disclosure of crimes against the peace and security of humanity, terrorism, corruption and organized criminal activity in the sphere of management and economy and other illegal actions that directly pose a threat to the vital interests of Ukraine.

The analysis of the law in the context of responding to crises threatening state security, the Security Service of Ukraine during the joint actions of the security forces performs, within the limits of their competence, the tasks defined by the Law by performing investigative actions and conducting service-operational measures.

The Law of Ukraine dated 07.02.2015 No. 580-VIII (as amended) states that the National Police of Ukraine (police) is a central agency of executive power that serves society by ensuring the protection of human rights and freedoms, countering crime, and maintaining public order, security and order.

According to this Law, the main tasks of the police are:

- ensuring public safety and order;
- protection of human rights and freedoms, and the interests of society and the state;
- countering crime;
- provision of assistance services to persons who, for personal, economic, or social reasons or as a result of emergency situations, need such assistance within the limits defined by law.

The police interact with law enforcement agencies and other state authorities, and local self-government agencies in the course of their activities.

The National Police performs the tasks assigned to it by the Law through the police system, which consists of the central police management agency and territorial police agencies.

The State Automobile Inspection supervises the observance of road safety rules, are obliged to regulate the movement of vehicles and pedestrians on the streets and highways. At the same time, the traffic police are obliged to monitor the technical condition of motor vehicles, its accounting, etc. Special police ensure public order in objects and territories that are of special importance or affected by a natural disaster, pollution, or disaster. The special purpose police (KORD) was created to solve emergency situations that are so dangerous, complex or unusual that they may exceed the capabilities of the emergency response forces or operational search units.

The National Guard of Ukraine is a military formation with law enforcement functions that is part of the system of the Ministry of Internal Affairs of Ukraine and is assigned to perform tasks of protecting the lives, rights, freedoms and legitimate interests of citizens, society and the state from criminal and other illegal encroachments, protecting public order and ensuring public safety, and in cooperation with law enforcement agencies to ensure state security and protection of the state border, stop terrorist activities, activities of illegal paramilitary or armed formations (groups), terrorist organizations, organized groups and criminal organizations. That is, in the process of responding to peacetime crisis situations, the National Guard is part of the security forces. However, during a special period (wartime), the NGU participates, under the law, in cooperation with the Armed Forces of Ukraine in repelling armed aggression against Ukraine and liquidating the armed conflict by conducting military (combat) actions, and performing territorial defense tasks, that is, acts as part of the state defense forces.

During responding to crisis situations that threaten state security, under the law-assigned functions, the National Guard of Ukraine ensures the protection and life's protection, rights, freedoms and legitimate interests of citizens, society and the state from criminal and other illegal encroachments, public safety and protection of public order, protection of state authorities. The functions of the National Guard of Ukraine have various vectors *(Horbulin V., Kachynskyi B., 2007)*.

The State Border Service of Ukraine is a special law enforcement agency tasked with ensuring the inviolability of the state border and protecting the sovereign rights of Ukraine in its adjacent zone and exclusive (maritime) economic zone.

To the authorities, units, military personnel, as well as employees of the State Border Guard Service of Ukraine who, according to their official duties, may be involved in operational and service activities related to the implementation of tasks assigned to the State Border Guard Service of Ukraine in responding to crisis situations threatening state security.

Thus, the State Border Guard Service of Ukraine is involved in joint actions with security forces in responding to crisis situations exclusively in border regions of the country and performs tasks to ensure the inviolability of the state border of Ukraine.

According to the Civil Protection Code of Ukraine, civil protection is a function of the state aimed at protecting the population, territories, natural environment, and property from emergencies by preventing such situations, eliminating their consequences, and providing assistance to the affected population in peacetime and in times of special periods. Depending on the nature of events, emergencies are classified into the following types: technogenic, natural, social, and military. Depending on the scale, emergencies are classified into the following levels: national, regional, local, and object. It should be noted that this classification of emergencies is fully consistent with our proposed classification of crises threatening state security.

The implementation of state policy in the field of civil protection is carried out by a unified state civil protection system, regulated by the resolution of the Cabinet of Ministers of Ukraine dated January 9, 2014, No. 11. The direct management of the activities of the unified state civil protection system is carried out by the State Emergency Service of Ukraine. The single state civil protection system consists of permanently operating functional and territorial subsystems and their elements.

The civil defense forces of the unified state civil protection system include: the operational rescue service of civil defense; emergency rescue services; civil defense formations; specialized civil defense services; fire and rescue units (subunits); voluntary civil defense formations.

Based on the classification of functioning regimes of the unified state civil protection system outlined in the Regulations, in our opinion, the tasks of the State Emergency Service of Ukraine (SES) in responding to crises threatening state security can be identified as follows:

– alerting the management authorities, civil defense forces, and the population about the occurrence of a crisis (emergency) situation and informing them about the actions to be taken in such conditions;
– determining the crisis situation zone;
– continuous forecasting of the possible spread zone of the crisis (emergency) situation and the

scale of possible consequences;

– organizing works to localize and eliminate the consequences of the crisis (emergency) situation, mobilizing necessary forces and resources for this purpose;

– organizing and implementing measures for the life susteinance of affected population;

– organizing and conducting evacuation measures (if necessary);

– organizing and implementing radiation, chemical, biological, engineering, and medical protection of the population and territories from the consequences of an emergency situation;

– continuous monitoring of the development of the crisis (emergency) situation and the situation at emergency sites and adjacent territories.

– informing the management of civil protection and the population about the development of a crisis (emergency) situation and the measures being taken.

The Armed Forces of Ukraine, other military formations and law enforcement agencies of special purpose may be involved in the work of elimination of the consequences of crisis (emergency) situations, which are carried out in the unified state system of civil protection. Public associations may be involved as well on a voluntary or contractual basis. It must be provided that the participants involved in such kind of work have an appropriate level of training.

The basis of the mechanisms for responding to crisis situations threatening state security is the system of ensuring internal security, which includes the system of ensuring public security and the civil defense system. In accordance with the hierarchical level of security management, security forces and public authorities perform tasks related to responding to crisis situations threatening state security. A feature of the presented mechanism is the activization of the activities of public organizations and associations of citizens in the system of ensuring state security in response to crisis situations at both national and regional and local levels. Non-state control over the activities of government agencies is an effective mechanism for preventing the excessive use of force at all levels of management listed above.

It should be noted that the research on the development of organizational and administrative mechanisms of state management through joint actions of security forces of Ukraine in response to crisis situations has not been conducted properly. At the same time, the contribution of individual scientists to the study of the problem is indisputable. For example, A.O. Diehtiar and S.V. Bielai in their scientific article studied state mechanisms to counteract crisis phenomena of socio-economic nature in Ukraine. The methodological aspect of forming such mechanisms was considered, a number of scientific and applied tasks were formulated, a methodology was provided, and a logic scheme for the corresponding research was formed.

By the Decree of the President of Ukraine dated March 14, 2016, No. 92/2016 “The Concept

of the Security and Defense Sector of Ukraine Development" it is stated that one of the main ways to achieve the necessary operational and other capabilities of the components of the security and defense sector is "creating a unified system of situational centers of state bodies that are part of the security and defense sector, as well as other government bodies at the national and local levels, ensuring its effective coordination using the capabilities of the Main Situation Center of Ukraine, creating conditions for the interaction of this system with the NATO Situation Center (SITCEN)" *(Horbulin V., Kachynskyi B., 2007).*

The genesis of the actions of security forces of Ukraine during crisis situations within the paradigm of state security. A sufficient level of the state military-economic potential is the basis for safeguarding its national interests and is also one of the main indicators for assessing the level of the state military security in general. It is widely known that the security of the state against internal and external threats is based on its military-economic strength. Sufficient military-economic potential of the state constitutes its defense capability. In turn, defense capability depends on the level of armament, military and special equipment, material and financial resources of the security and defense forces. The task of creating the necessary level of provision for the security and defense forces is the major task of the state military economy. The ability of the state to provide for its military needs economically is one of the main components of defense capability.

Thus, one of the main tasks of the state leadership is to maintain a sufficient level of military-economic security. This task has a dialectical contradiction, namely, to prevent a decrease in defense capability on the one hand, and to avoid exceeding defense spending on the other hand. During crisis situations, there is a need to increase spending on security and defense forces, which can lead to a decrease of the state economic indicators. The task of increasing resource provision for security forces during crisis situations must be rational.

The part of the economic potential of a country used to satisfy the needs of its security forces in armaments and military equipment constitutes the military-economic potential. This indicator characterizes the military-economic capabilities of the country, forming a component of the state defense capability.

Another indicator characterizing defense sufficiency is the country's GDP. This indicator reflects the results of the state economic activity at the macro level, meaning the total market value of final goods and services produced by enterprises, organizations, and institutions in the country's economic territory throughout a year. An analysis of the GDP dynamics of some countries worldwide for the years 2012-2021 indicates that the growth has ranged from 3% to 7% during the examined years *(Semenenko O., Taran O., Tregubenko S., Onofriychuk P., Pekulyak R., Motrunych I., 2022).*

China has demonstrated the highest GDP growth rate in the world in recent years, with an

average indicator of approximately 9%. Countries with stable economies and developed industries show GDP growth rates of up to 4%. These countries include the USA, Great Britain, Germany and France *(Semenenko O., Boyko R., Vodchits O., Dobrovolsky Yu., Berdochnik D., Yaroshenko A., 2017)*.

The significant growth of China's GDP is due to revolutionary growth of innovative technologies in industry, an increase in the number of enterprises, state support for the scientific and technical potential of the country, and low labor costs. This creates conditions for the competitiveness of the Chinese production.

The growth rates of Russia's GDP are driven by significant development of the defense-industrial complex, state support for the scientific and technical potential of the country, and the increase in prices of natural resource raw materials in international markets *(Semenenko O., Taran O., Tregubenko S., Onofriychuk P., Pekulyak R., Motrunych I., 2022)*. The high GDP growth rates of the USA have a stable character due to the development of the defense-industrial complex, a consistent policy of reducing external debt and budget deficit, innovative technologies in the IT sector, and advanced scientific research.

In the countries neighboring with Ukraine, there has also been an average GDP growth of 3.3% from 2012 to 2020. In 2018, Belarus' GDP increased by 3% due to the development of processing industries (forming 21.5% of GDP), with growth rates reaching 5.4% *(Semenenko O., Taran O., Tregubenko S., Onofriychuk P., Pekulyak R., Motrunych I., 2022)*.

Leading economies in Europe have experienced a decline in GDP growth rates over the past 10 years, leading to problems with meeting obligations regarding defense spending, which should be at least 2% of GDP, with 20% allocated for development programs and procurement of new weapons and military equipment.

In 2023, India took the fifth place among all countries in the world and the second one among the developing countries (after China) in terms of nominal GDP ($3.47 trillion). The state GDP has been continuously growing at a rate of 7% according to the results of 2022-2023.

Besides the key indicators, characterizing the state of a country's GDP and the level of its defense capability, the indicator of defense spending should be taken into account. The analysis of defense spending in leading countries worldwide shows (Figure 1, Figure 2), that the European countries and the USA have been reducing their defense expenditures. However, in the current complex geopolitical conditions, starting from 2014, these countries are trying to restore defense sector funding to the levels of 2007-2008.

Figure 1.

GDP Rates of Some Countries of the World (USD bln)

Years Country	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
USA	16 197	16 784	17 521	18 219,3	18 707,2	19 485,4	20 544,3	21 439,4	19 332,1	20 240,7
Germany	3 527,3	3 732,7	3 883,9	3 360,5	3 466,8	3 656,75	3 947,62	3 863,34	3 671,28	3 862,19
France	2 683,8	2 811,1	2 852,17	2 438,21	2 471,29	2 586,29	2 777,54	2 707,15	2 577,55	2 693,54
Russia	2 210,2	2 297,1	2 059,98	1 363,59	1 282,72	1 578,62	1 657,55	1 637,89	1 566,38	1 621,20
China	8 532,2	9 570,4	10 438,5	11 015,5	11 137,9	12 143,5	13 608,1	14 140,1	13 771,4	15 038,4
Britain	2 704,9	2 786	3 063,8	2 928,59	2 694,28	2 666,23	2 855,30	2 743,59	2 726,81	2 868,60
Belarus	65,69	75,53	78,81	56,45	47,72	54,73	60,03	62,57	56,42	59,98
Poland	500,36	524,23	545,39	477,58	472,03	526,22	585,66	565,85	558,71	582,18
Turkey	873,98	950,58	934,19	859,80	863,72	852,68	771,35	743,71	732,78	769,42
Romania	171,20	190,95	199,63	177,89	188,49	211,70	239,55	243,7	227,57	236,44

Europe has understood the danger of underfunding the defense sector. According to the NATO Secretary General Anders Fogh Rasmussen, “freedom does not come for free, and any decision made to improve our economy should not plunge us into another type of crisis – a security crisis” *(Semenenko O., Taran O., Tregubenko S., Onofriychuk P., Pekulyak R., Motrunych I., 2022)*. Against the backdrop of reductions in defense spending by the European and US countries, countries like China and Russia have annually increased their spending by an average of 20-30% compared to previous indicators. These indicators exist due to increased funding for the defense-industrial complex, intensification of scientific research, and increased demand for advanced weaponry, military, and special equipment.

In countries like Turkey, the increased defense spending is driven by the need for rearmament and corresponding personnel retraining. In Poland and Romania, the increased spending is driven by raising the social status of military personnel and also the level of readiness of their armed forces. In Belarus, the growth in defense spending is caused by increased spending on the operation of weapons, military and special equipment, and the rising cost of energy resources, that increase expenditure on combat training [*(Semenenko O., Boyko R., Vodchits O., Dobrovolsky Yu., Berdochnik D., Yaroshenko A., 2017)*.

Figure 2

Defense Expenditures in Some Countries of the World (USD Bln)

Country	Value of indicators by year								
	2012	2013	2014	2015	2016	2017	2018	2019	2020
USA	725,205	679,229	647,789	633,83	639,856	646,753	682,491	732,00	750,00
Germany	44,47	44,866	44,216	37,02	39,725	42,366	46,512	49,30	45,05
France	50,217	52,002	53,135	45,648	47,37	49,196	51,41	50,10	59,54
Russia	81,469	88,353	84,697	66,418	69,245	66,527	61,388	65,10	66,00
China	157,39	179,881	200,772	214,472	216,404	228,466	253,492	261,00	278,22
United Kingdom	58,496	56,862	59,183	53,862	48,119	46,433	49,892	48,70	46,88
Belarus	0,817	0,971	1,011	0,724	0,597	0,631	0,715	0,75	0,55
Poland	8,987	9,276	10,345	10,213	9,164	9,871	12,041	11,90	11,23
Turkey	17,694	18,428	17,577	15,669	17,828	17,823	19,649	20,40	19,00
Romania	2,103	2,453	2,692	2,581	2,644	3,622	4,359	4,90	4,55

In these countries, defense expenditures range from an average of 3% to 8% of GDP. Other European countries pursued a policy of cost-saving on defense, and their GDP showed unstable trends from year to year, which have also destabilized the security environment in Europe and created an imbalance on this issue globally.

Figure 3 shows defense expenditures of leading countries of the world as a percentage of GDP. One of the main goals of Ukrainian military policy is to prevent military conflicts. One of the ways to prevent such conflicts is to ensure the combat readiness of security and defense forces at a level sufficient to deter a potential aggressor from using the military force against Ukraine. Research of the Ukrainian legislative framework for ensuring the state defense capability shows that it relies upon the Armed Forces, their level of proficiency, equipment, and training, determine its defense sufficiency.

One of the factors influencing on the state security is its defense potential. Achieving the necessary defense potential of the state is ensured by the development and improvement of its military organization, as well as providing for its development through the allocation of sufficient financial, material, and other resources.

The scale and complexity of crises that arise in the state today, require adjustments to the tasks of security forces and the development of rational response scenarios to these situations. Security force response scenarios to crisis situations require the formation of factors within the state

governance system, that would lead to the effective and timely execution of these tasks. One of these factors is the formation of a rational defense budget.

Figure 3

Defense Expenditures of Leading Countries of the World (% of GDP)

Country	Value of indicators by year								
	2012	2013	2014	2015	2016	2017	2018	2019	2020
USA	4,48	4,05	3,7	3,48	3,42	3,32	3,32	4,48	3,79
Germany	1,26	1,2	1,14	1,1	1,15	1,16	1,18	1,26	1,34
France	1,87	1,85	1,86	1,87	1,92	1,9	1,85	1,87	1,94
Russia	3,69	3,85	4,11	4,87	5,4	4,21	3,7	3,69	4,16
China	1,84	1,88	1,92	1,95	1,94	1,88	1,86	1,84	1,90
United Kingdom	2,16	2,04	1,93	1,84	1,79	1,74	1,75	2,16	1,79
Belarus	1,24	1,29	1,28	1,28	1,25	1,15	1,19	1,24	1,33
Poland	1,8	1,77	1,9	2,14	1,94	1,88	2,06	1,8	2,13
Turkey	2,02	1,94	1,88	1,82	2,06	2,09	2,55	2,02	2,78
Romania	1,23	1,28	1,35	1,45	1,4	1,71	1,82	1,23	2,15

Some researchers consider that exceeding defense spending will have a negative impact on the development of the national economy. This viewpoint can be agreed upon, especially during peacetime. During crises, defense expenditures directly affect national security. Neglecting the needs of security forces in all aspects of provisioning will have a negative impact on the overall national security of the country. A rational defense budget in peacetime lays the groundwork for effective methods of security force response to crisis situations. Thus, the effective execution of security force response tasks during crisis situations relies on a balance between provisioning needs and expenditures.

Factors influencing on the state defense sufficiency (its ability to respond to crisis situations) can be divided into internal and external factors. Internal factors include political, military, economic, sociocultural, demographic, spiritual, temporal, informational factors, etc. These factors form the basis of a state military-economic power. These factors must be considered while provisioning security forces with material and technical resources. It is impossible to ignore the impact of external factors on national security. External factors, depending on their properties and the degree of influence on the level of the state defense sufficiency, can be grouped into the following categories: geographic, economic, political, military, religious, ethnic, informational, ecological, etc. The

military-political goals of a country are determined by the properties of external factors.

It's essential to consider the impact of economic factors on the security component of the state.

The functions of the economy in ensuring national security include:

1. Analysis of the economic situation, forecasting its development, synthesizing long-term plans for industrial development, developing concepts for the development of security force military-industrial complex, investing in prospective economy sectors.

2. Implementing well-developed plans into the defense-industrial sector, ensuring the execution and control of tasks at all levels of state management.

3. Mobilizing all types of resources for the realization of military, social, and economic development tasks.

The military-economic development of a country during crisis situations is primarily aimed at ensuring its security based on the effective use of defense capabilities and fostering the development of mobilization capabilities. The goal of military-economic development during crises is to create security forces capable of effectively performing state-assigned tasks with the necessary efficiency, having the combat and mobilization readiness sufficient for preventing and overcoming crisis situations which are caused by both external and internal factors. Means to achieve this goal may include: intensifying scientific and technological progress in developing advanced weapons systems and military equipment through additional funding for fundamental research; changes in approaches to provide scientific personnel; reforming and changing approaches to ensure military-technical training; transitioning to the NATO standards; creating an effective and transparent management and control system for task execution; reducing corruption risks; creating an effective system of military procurement and supply.

The combat readiness of security and defense forces of Ukraine is their ability to initiate military actions and accomplish assigned tasks successfully under any conditions within established timelines. The degree of equipment with military equipment, weapons, personnel training for task execution, and the state of morale and psychological support constitute the level of combat readiness of security and defense forces of Ukraine. The execution of tasks assigned to security forces mostly depends on the degree of organization of their activities, operation, modernization, repair of military equipment, funding for restoring combat readiness. Hence, one of the mechanisms of state management in the technical support system is material and technical support for security forces. Another mechanism of state management is normative-legal regulation of the technical support system for security forces. This mechanism includes laws, concepts, programs, and strategies for the development of technical support for security forces.

At the current stage of the country's development, security forces are formed based on the

developed concepts and programs that determine the modern policy of the state. This is reflected in the defense nature of the military doctrine, with one of its main elements being the principle of defensive sufficiency. Defensive sufficiency for security forces primarily represents their capabilities to overcome threats to national security. These capabilities are built on organizational and staff structure, material and technical support, morale and psychological state, and personnel readiness. The principle of defensive sufficiency is comprehensive, incorporating political, military, technical, and economic elements.

The solution of synthesizing an optimal military-economic strategy of the state lies in creating a balance between the military needs of security and defense forces and the socio-economic needs of society. Such a balance is possible through the optimal allocation of resources and rational planning for the development of security and defense forces. Creating such a balance during crisis situations is challenging because security issues are prioritized, without which resolving socio-economic issues make no sense.

The interaction between elements of defense sufficiency can be represented as follows *(Semenenko O., Taran O., Tregubenko S., Onofriychuk P., Pekulyak R., Motrunych I., 2022)*:

– Ukraine's accession to NATO, the establishment of foreign policy agreements on security guarantees;

– building a security and defense force structure that would be optimal for addressing set tasks and ensuring the sufficient level of the state defense capability;

– changes in the structure of security and defense forces will lead to changes in comprehensive defense provision for the country;

– changes in comprehensive defense provision for the country will lead to the review of views on the military budget of the country, the principles of creating strategic reserves, mobilization readiness;

– the degree of provision of Ukrainian security forces depends on the capabilities of the defense-industrial complex and the quality and speed of deliveries (procurements) of military equipment.

The implementation of principles of defense sufficiency allows revealing the directions of defense aspects in the military-economic strategy of the state. In modern conditions of Ukraine's development, during armed aggression by the Russian Federation, the principles of building security and defense forces, their comprehensive provision, mobilization readiness, armament, military and special equipment need to be revised. Undoubtedly, the military power of the state is based on its economic potential, resource provision (both industrial and human). Planning for the development of Ukraine's security and defense forces must be carried out, considering the priority directions for ensuring the necessary level of defense sufficiency of the future type of Ukrainian security and

defense forces. It is necessary to determine the directions for achieving the planned result in the long term.

The most important component of defense significance nowadays is the need to ensure Ukraine's security and defense forces with weapons and military equipment. The armament and military equipment which are currently in service with the security and defense forces of Ukraine have a wide range. But some samples are outdated, and their reliability indicators are reduced due to the lack of major repairs and operating conditions. Updating of the armament, military and special equipment is possible under the conditions of improvement of centralized supply, simplification of procurement procedures, acceleration of scientific and technical research. This can be achieved with the help of rational long-term planning with a single strategic intent, which constitutes a system of economic and organizational measures aimed at creating the most favorable conditions for the development of science and the implementation of its results in new equipment and technologies. The development of these measures should aim at the development of armament, military and special equipment, the implementation of developed plans for their creation, procurement, and production, operational and technical support for high combat readiness of security and defense forces *(Semenenko O., Taran O., Tregubenko S., Onofriychuk P., Pekulyak R., Motrunych I., 2022).*

Scientific and technical research under a long-term development plan for armament, military and special equipment should meet the following requirements:

- determining the priority means of armament, military and special equipment that will allow solving strategic and operational-tactical tasks regarding the defense of the state, having the greatest impact on the effectiveness of performing such tasks;

- determining the rational composition of armament, military and special equipment for each type of security and defense forces of Ukraine, taking into account their capabilities for interaction in operations;

- ensuring the development, production, procurement of new models of armament, military and special equipment, taking into account new enemy tactical methods, their strategy of combat operations;

- modernization of armament, military and special equipment.

As confirmation of the dependence of the war outcome (combat operations) on the level of material and technical support and production, one can trace the example of the military-economic confrontation between the USSR and Germany during the years of the World War II.

Military economy as a specific part of the national economy has a complex structure. In general, it consists of defense (military) industries; basic sectors of the national economy in terms of providing the defense industries with means of production, and labor resources of the military economy and

personnel of the armed forces as consumers; transport, communication, material and technical supply systems, as well as science, healthcare, education in terms of servicing the production of military products and the functioning of the Armed Forces.

The combat capability of the security and defense forces of a state is significantly determined by the level of their technical equipment. Activities in the military-technical field, aimed at organizing comprehensive, coordinated efforts in terms of objectives, tasks, resources, and time frames for ensuring timely and full provision of security and defense forces with modern samples, complexes, and systems of armaments, military and special equipment. This activity is implemented through the implementation of state military-technical policy, which encompasses a range of measures related to the development planning, design, modernization, production, procurement, and supply to the troops, repair, and maintenance of armaments, military and special equipment, as well as the construction of facilities for equipment installation (placement), the development of the scientific, industrial, and technological base of defense industries.

One of the main tasks, the solution of which is oriented to the state military-technical policy, is the support in the combat-ready state of weapon samples, military and special equipment, which are used in the Armed Forces, and the development of the armament system of the security and defense forces in accordance with the tasks assigned to them, primarily based on the analysis and forecasting of threats to national security in the military sphere and the economic capabilities of the state.

The armament system of the security and defense forces is a balanced multilevel organizational and technical system, represented as a set of samples, complexes, and systems of armaments, military and special equipment of various types and kinds, functionally related and organizationally arranged in the structure of the security and defense forces, distributed among the staffed military formations in accordance with their purpose and coordinated by the ratio of means of combat management, combat and technical support, nomenclature, quantitative composition, functions performed, and the level of tactical and technical characteristics to ensure the effective implementation of combat tasks by the Armed Forces in combat and daily activities.

It includes a wide range of samples (complexes, systems) of armaments, military and special equipment of various types and kinds that are in service with military formations, which have a certain combat composition and staff structure, equipped with specific samples of armaments, military and special equipment, functionally related by tasks performed, and organizationally combined in the formations of security and defense forces intended to perform tasks of general strategic, strategic, operational-strategic, operational-tactical, and tactical levels. The main elements of such an armament system are weapons, control means, and support means.

One of the fundamental properties of the armament system of the security and defense forces

as a complex organizational and technical system is its natural decomposability, which allows it to be represented as a balanced multilevel hierarchical structure with links between the components of the system, adequate to the organizational-structural and functional links between the organizational military formations of the security and defense forces. The goals, tasks, principles, and main directions of development of the armament system of the security and defense forces are determined by its purpose and reflected in the concept of the development of armaments, military and special equipment.

The development and maintenance of the armament system and its components in a combat-ready state is carried out within the framework of the technical equipment of the security and defense forces, which represents a set of coordinated measures aimed at planning and managing the development of the armament system, design, production, procurement, and supply to the troops, ensuring operation and repair of samples of armaments, military and special equipment, as well as the supply of component products, ammunition, consumables, etc.

The main mechanism for solving tasks in the field of technical equipment of the security and defense forces is the development (justification and formation) and implementation of a set of program and planning documents, including: a state program and plans for the construction and development of the armed forces; state armament program; state defense order; targeted and other programs and plans related to the sphere of military construction as a whole and military-technical support of defense and security of the state in particular.

These documents are created based on pre-formed initial data of military-political, operational-strategic, military-economic, military-technical, and other nature.

The state armament program is aimed at ensuring the solution of tasks determined by the state program for the construction and development of the security and defense forces in favor of increasing defense capability and state security.

To address the issues of technical equipment for security and defense forces and the development of their armament systems, three main approaches can be used: evolutionary, revolutionary, and combined, which rationalizes the first two approaches.

The evolutionary path is based on systematic and gradual (evolutionary) technical rearmament of security and defense forces with extensive use of life extension of existing weapon samples, military and special equipment through their improvement and modernization. It is less costly than creating new weapon samples, military, and special equipment, and is widely used in world practice. However, this path has significant drawbacks associated with the limited potential reserve of modernization of weapon samples, military, and special equipment, which is laid down during their development, as well as with the incomplete use of scientific and technical progress achievements

and lagging behind in the development of forms, methods, and means of the armed struggle.

In terms of armament system renewal the second (revolutionary) approach to the technical rearmament of security and defense forces is more progressive. It involves the accelerated development of new-generation weapon samples, military and special equipment with subsequent deployment of their full-scale production at a high pace of armament system renewal. The progressiveness of this approach, along with the noted character of more intensive increase in the level of equipping security and defense forces with modern weapon samples, military, and special equipment, is also manifested in strengthening the country's position in the world arms market. The latter is very important not only from a political point of view but primarily from an economic point of view, allowing part of the income received from arms trade to be directed towards the country's own defense needs. However, in general, the revolutionary approach proves to be very costly and, with its widespread (massive) application, it requires a high strain on the state economy.

In conditions of limited possibilities for financing the development of armaments, military, and special equipment, a more preferable (priority) approach for supporting the combat readiness of security and defense forces from a technical point of view may be recognized as a combined approach, which rationally combines the modernization and life extension of existing weapon samples, military, and special equipment with the development (albeit very costly) of new samples. The main limiting factor, along with additional expenditures of financial resources, in this case is the availability and condition of the corresponding research and design and production-technological base of the country. The level of development of this base must lead to the creation of new pre-planned samples, which can be implemented with the minimal risk.

Thus, in conditions of the absence of large-scale military threats and favorable forecast assessments of the military-political and military-strategic situation in the near (planned) perspective, it is advisable to carry out the technical rearmament of security and defense forces and maintain their armament system in combat-ready condition through modernization and extension of the service life of weapon samples, military, and special equipment, simultaneously creating a reserve for individual promising samples within the financial-economic capabilities of the country without cumbersome temporary and financial intensification of work on the technical equipment of security and defense forces.

From the standpoint of an operational-strategic approach for building the armament system of security and defense forces, it is represented as a set of functionally related armament systems of military formations designed to solve the corresponding tasks of the general strategic, strategic, operational-strategic, operational-tactical, and tactical levels, that is, all levels of the tasks system of security and defense forces. This approach to forming the armament system of security and defense

forces necessitates the conduct of operational-strategic justification of its development prospects based on the results of analysis and forecasting of the military-political situation, the possible composition of opposing security and defense forces, and their technical equipment, taking into account the limitations imposed by the adopted military doctrine. This necessitates the development of forecasts for the content and duration of possible wars, scenarios of operations, and combat actions. The obtained data should ensure the correlation of operational-strategic tasks of security and defense forces (taking into account the forms and methods of their solution) and armament systems of regular military formations designed to address these tasks.

From the standpoint of a military-technical approach, the armament system of security and defense forces is divided into subsystems of strategic, operational-strategic, and operational-tactical armaments, with further differentiation based on organizational-structural features into subsystems of armaments of types of security and defense forces, branches of troops, and further detailing into types and models of specific armaments, military, and special equipment. At the same time, the military-technical approach allows for the integration of different types and models of armaments, military, and special equipment, combat assets, control means, and support means within functionally closed subsystems designed to address specific military-technical tasks.

The military-technical approach allows to present the prospective armament system of security and defense forces as a rational set of functionally closed subsystems, including combat and support assets, designed to address specific military-technical tasks. The accomplishment of these tasks within the framework of corresponding operations ensures the solution of operational-strategic tasks faced by security and defense forces in possible crisis situations. The military-technical approach is based on viewing armaments, military, and special equipment as means of fulfilling military-technical tasks, the essence of which primarily lies in the destruction or disabling of enemy objects.

In general, the alignment of the tasks system of security and defense forces and their armament systems, carried out using operational-strategic and military-technical approaches, allows to identify objectively existing links in the following chain: operational-strategic tasks of security and defense forces → military-technical tasks of the armament system of security and defense forces → functionally closed subsystems of armaments, military, and special equipment → state program of armaments development → state defense order.

The choice of directions for the development of armaments, military, and special equipment and technical rearmament of security and defense forces in the considered program period should be based on a comprehensive consideration of military-political, operational-strategic, military-technical, and military-economic factors. This requires further improvement of the scientific-methodological apparatus for justifying the main directions of armaments development, military, and

special equipment, and armament programs, taking into account the main trends in the development of forms, methods, and means of the armed struggle.

The basis of the process of technical rearmament of security and defense forces is measures for the creation and supply of prospective and modernized samples of armaments, military, and special equipment instead of existing ones that do not meet modern requirements. The military-technical aspect of equipping and re-equipping security and defense forces is associated with the capabilities for joint effective combat use of basic, basic modernized, modernized, and prospective samples of armaments and military equipment. The samples of armaments and military equipment participating in this process are divided into developed and existing samples.

The functioning of security and defense forces consists of two interconnected processes:

- the application of security and defense forces for their intended purpose, i.e., the deployment and use of special elements of formations – troops (forces) to address the country's defense tasks, characterized by the consumption of previously accumulated combat potential (various resources: trained personnel, special technical means, and materials);

- construction of security and defense forces, which includes creating, accumulating, and maintaining a designated combat potential through the implementation of a special complex of measures regarding the training and accumulation of human resources, procurement of weaponry samples, military and special equipment, construction and maintenance of infrastructure facilities, and accumulation of material resources.

The resource base of security and defense forces consists of the following resource groups: organizational resources; personnel resources; technical resources; material resources.

The basic systems of security and defense forces are as follows:

- security and defense forces management system;
- system of operational, combat, and mobilization training of troops (forces);
- mobilization deployment base of security and defense forces;
- system of security and defense forces personnel staffing and training;
- armed forces technical support system;
- comprehensive logistical support system for security and defense forces;
- system of deployment and basing of military formations;
- infrastructure support system for security and defense forces;
- system of financial support for security and defense forces;
- military communications system.

In the interests of ensuring the functioning of security and defense forces, systems of state reserve, mobilization deployment, country mobilization training, and defense industry are being

created. It facilitates the transition of security and defense forces from peacetime to a state of full combat readiness for deployment.

Within the framework of the technical support system for security and defense forces, measures are taken for creation and supply (procurement) of weaponry samples, military and special equipment and putting them into operation, ensuring the planned operation, modernization, military and capital repairs of weaponry samples, military and special equipment, accumulation and storage, withdrawal from combat inventory, and subsequent disposal. Moreover, various types of technical support for troops (forces) are implemented within this system, determined by the existing range of weaponry samples, military and special equipment, and the rules of their technical operation and application. The necessary scope of the listed measures, in turn, is determined by the dynamics of the technical condition and the level of functional efficiency of existing weaponry samples, military and special equipment, as well as the parameters of the prospective appearance of security and defense forces.

Long-term and medium-term planning documents in the field of construction and development of security and defense forces can be grouped into two categories: resource provision and organizational-administrative management.

The group of documents regarding resource provision includes:

– state armament program;

– program of resource provision for measures of operational, combat, and mobilization training of security and defense forces;

– program of development of security and defense forces infrastructure, including operational equipment of the country's territory and construction of facilities for weapon mounting, military and special equipment;

– program of formation of material resources for logistical and financial support of security and defense forces.

The group of documents on organizational-administrative management includes:

– state program of construction and development of the Armed Forces;

– equipment (re-equipment) program for armament, military and special equipment of units and parts of security and defense forces, including a plan for withdrawing armament, military and special equipment from combat inventory;

– program of operational, combat, and mobilization training of security and defense forces;

– program of enhancing the foundation of security and defense forces;

– program of forming personnel resources of security and defense forces.

The system of program planning documents in the field of construction and development of security and defense forces should ensure the coherence of the objectives of military construction

with the resource capabilities of the state. It is advisable to develop a state program for the construction and development of security and defense forces in the form of two documents: the main parameters of the construction of security and defense forces and the calculated justifications for the parameters of the construction of security and defense forces.

The main parameters of the construction of security and defense forces should include the values of indicators of their external appearance and volumes of allocations directed towards their achievement.

In turn, the calculated justifications for the main parameters of the construction of security and defense forces should contain a list of general construction measures and their parameters. They should allow assessing the correctness of the values of the declared parameters of the construction of security and defense forces, be the target guidelines for the formation of resource programs and programs of organizational and administrative management.

Conclusions. Based on the stated above, the following can be concluded.

1. The role and place of security forces of Ukraine in response to crisis situations have been studied. The genesis of the security forces of Ukraine actions during crises in the paradigm of state security has been characterized. Regulatory legal acts in the field of ensuring national security have been considered. The definition of a “crisis situation" has been examined. The analysis of regulatory legal documents allows to state that a new term “crisis situations threatening the national security of Ukraine” has been introduced, which characterizes the situation on the eve of the introduction of a special period. It has been determined that in the system of ensuring national security, the main subjects of ensuring state security are security forces.

2. An assessment of the level of military security of the country based on the level of the military-economic potential of the state, which is the basis of protecting its national interests, has been carried out. The main economic indicator that can characterize the state of military-economic policy of the state and the level of its defense sufficiency is the GDP indicator of the country. An analysis of the dynamics of the GDP of some countries of the world for 2012-2021 indicates that its growth during the years under study ranges from 3% to 7%. China is the leader in the GDP growth rate (average indicator is about 9%). The USA, Germany, France, and Great Britain maintain their leadership positions in the economy, and the growth rates of their GDP have remained standard and most acceptable at about 4%, which is a sign of economic stability and adherence to classical schemes of its development. 3. Military potential depends on the degree of saturation with weapons, military and special equipment of security and defense forces. The speed of production and restoration of weapons, military and special equipment will be the main feature of the military potential of the state. One of the requirements for security forces is the requirement of balance, which is expressed in

establishing rational proportions among different types of weapons. In each country, these proportions are established taking into account the features of the military doctrine, the specificity of the tasks assigned to the Armed Forces, the levels of development of technology, historical traditions, and other factors.

4. Common views on the nature of possible military actions and the proximity of tactical and technical characteristics of weapons in leading countries of the world lead to the fact that differences between their armies are largely leveled, and the ratio of different types of armaments turns out to be close. At the same time, the ratio of armaments practically does not depend on their quality and the total number of armies. It depends little on the political situation in the world. All the aspects mentioned above allow us to interprete these results as regularities of armaments systems, military and special equipment development.

References:

Babkov Yu.P., AdamchukM.M. (2016). Pidkhody do pryiniattia rishen pry reahuvanni na kryzovi sytuatsii, shcho zahrozhuiut natsionalnii bezpetsi Ukrainy. Stan ta perspektyvy reformuvannia sektoru bezpeky i oborony Ukrainy [Approaches to making decisions in responding to crisis situations that threaten the national security of Ukraine. Status and prospects of reforming the security and defense sector of Ukraine]. *Materialy mizhnar. nauk.-prak. konf. – Materials from the conference*. (pp.24-27) K.: «PALYVODA A.V.» [in Ukrainian].

Basov, A.V. (2010). Shchodo vyznachennia systemy zabezpechennia hromadskoi bezpeky [Regarding the definition of the public safety system]. *Forum prava – Law forum*, 4, 42-47 [in Ukrainian].

Belay, S.V. (2015). *Derzhavni mekhanizmy protydii kryzovym yavyshcham sotsialno-ekonomichnoho kharakteru: teoriia, metodolohiia, praktyka [State mechanisms of counteraction to crisis phenomena of social and economic nature: theory, methodology, practice]*. Kharkiv: National Academy NGU [in Ukrainian].

Belay, S.V., & Bondarenko, O.G. (2017). *Udoskonalennia mekhanizmiv reahuvannia na kryzovi sytuatsii, shcho zahrozhuiut derzhavnii bezpetsi Ukrainy. Protses modernizatsii systemy derzhavnoho upravlinnia: administratyvnyi, ta finansovyi aspekty [Improvement of mechanisms of response to crisis situations that threaten the state security of Ukraine. The Process of Modernization of the Public Administration System: Administrative and Financial Aspects]*. Odessa: Publishing house "Helvetica" [in Ukrainian].

Bondar, O. V. (2012). *Sytuatsiinyi menedzhment [Situational management]*. K.: Tsentr uchbovoi literatury [in Ukrainian].

Didivska, L.I., & Golovko, L.S. (2007). *Derzhavne upravlinnia ekonomiky [State Management of Economy]*. K.: Znannia [in Ukrainian].

Horbulin, V.P., & Kachynskyi, A.B. (2007). *Systemno-kontseptualni zasady stratehii natsionalnoi bezpeky Ukrainy [Systemic and conceptual principles of the national security strategy of Ukraine]*. K.: Yevroantlantikinform [in Ukrainian].

Mashkov, O. A., & Nizhnik, N. R. (1998). *Systemnyi pidkhid v orhanizatsii derzhavnoho upravlinnia [System approach in the organization of public administration]*. K.: UADU [in Ukrainian].

Ponomarenko H. O. (2007). *Upravlinnia u sferi zabezpechennia vnutrishnoi bezpeky derzhavy: administratyvno-pravovi zasady [Management in the field of ensuring the internal security of the state: administrative and legal principles]*. Kharkiv: FOP Vapniarchuk [in Ukrainian].

Reznikova, O.O. (2022). *Stratehichnyi analiz bezpekovoho seredovyshcha Ukrainy [Strategic*

analysis of the security environment of Ukraine]. K.:Natsionalnyi instytut stratehichnykh doslidzhen. Retrieved from https://niss.gov.ua/news/statti/stratehichnyy-analiz-bezpekovoho-seredovyshcha-ukrayiny [in Ukrainian].
Semenenko, O., & Taran, O., Tregubenko, S., Onofriychuk, P., Pekulyak, R., Motrunych I. (2022). Osnovni teoretychni aspekty zabezpechennia oboronnoi dostatnosti derzhavy z urakhuvanniam stanu rozvytku yii natsionalnoi ekonomiky [Basic theoretical aspects of ensuring the defense sufficiency of the state, taking into account the state of development of its national economy]. *Journal of Scientific Papers "Social Development and Security"– Journal of Scientific Papers "Social Development and Security"*, 12(3), 54-59 [in Ukrainian].
Semenenko, O.M., & Boyko R.V., Vodchits O.G., Dobrovolsky Yu.B., Berdochnik D.V., Yaroshenko A.V. (2017). Osnovni metodolohichni aspekty voienno-ekonomichnoho zabezpechennia oboronozdatnosti derzhavy: teoriia ta praktyka [Basic Methodological Aspects of Military-Economic Support of State Defense: Theory and Practice. Information processing systems]. *Systemy obrobky informatsii – Information processing systems*, 3 (51), 165-175 [in Ukrainian].
Sytnik, G.P. (2012). *Derzhavne upravlinnia u sferi natsionalnoi bezpeky (kontseptualni ta orhanizatsiino-pravovi zasady) [State management in the field of national security (conceptual and organizational and legal principles)]* K.: NAPA [in Ukrainian].

DOI 10.5281/zenodo.10821974
UDC 621.316.5: 621.3

CHAPTER 15.
DEVELOPMENT OF CONTACT MATERIAL WITH INCREASED ENVIRONMENTAL SAFETY AND ELECTRO-EROSION RESISTANCE

Vasyl KOKHANOVSKYI
PhD in Engineering, Associate professor
Associate professor of Department of Printing Machines and Automated Complexes
Igor Sikorsky Kyiv Polytechnic Institute
(Kyiv, Ukrainę)
v.kokhanovskyi@kpi.ua
https://orcid.org/0009-0002-4804-884X

Abstract. In this study, the scientific methods of creating an environmentally safe composite contact material with increased electroerosion resistance for low-voltage switching electrical devices are substantiated. The resource of operation, reliability and environmental friendliness of electrical devices is improved due to the use of new developed silver-based contact materials in them.

To determine the type of admixtures that improve the operational characteristics of the contact material, their classification was carried out according to the nature of the effect on the contact properties of the material and the choice of the specified ingredients was substantiated, in accordance with the scientific principles of structuring of composite materials.

A comparative experimental study of magnetic starters with serial and experimental contact materials for switching wear resistance showed that the electroerosion resistance of experimental contact parts is 1.7 times higher than that of serial ones. The results of the work can be implemented in the industrial production of contact systems of switching electrical devices at domestic enterprises.

Key words: environmental safety, electrical devices, contact material, electrical erosion resistance, composite materials.

РОЗРОБКА КОНТАКТНОГО МАТЕРІАЛУ З ПІДВИЩЕНОЮ ЕКОЛОГІЧНОЮ БЕЗПЕКОЮ ТА ЕЛЕКТРОЕРОЗІЙНОЮ СТІЙКІСТЮ

Анотація. У даному дослідженні обґрунтовано наукові методи створення екологічно безпечного композиційного контактного матеріалу з підвищеною електроерозійною

стійкістю для комутаційних електричних апаратів низької напруги. Ресурс експлуатації, надійність та екологічність електричних апаратів покращується за рахунок використання в них нових розроблених контактних матеріалів на основі срібла.

Для визначення типу домішок, що покращують експлуатаційні характеристики контактного матеріалу, було проведено їх класифікацію за характером впливу на контактні властивості матеріалу та обґрунтовано вибір визначених інгредієнтів, згідно з науковими принципами структуроутворення композиційних матеріалів.

Порівняльне експериментальне дослідження магнітних пускачів із серійними і дослідними контактними матеріалами на комутаційну зносостійкість показало, що електроерозійна стійкість дослідних контакт-деталей в 1,7 рази вища, ніж у серійних.

Результати роботи можуть бути впровадженні при промисловому виготовленні контактних систем комутаційних електричних апаратів на вітчизняних підприємствах.

Ключові слова: екологічна безпека, електричні апарати, контактний матеріал, електроерозійна стійкість, композитні матеріали.

ВСТУП.

Електричні низьковольтні апарати з контактними комутаційними елементами становлять близько 90 % ринку комутаційних апаратів завдяки суттєвим перевагам над апаратами з напівпровідниковими комутаційними елементами: глибина комутації, перевантажувальна здатність, малі втрати енергії, стійкість до коротких замикань тощо.

Одним із розповсюджених видів комутаційних апаратів і апаратів керування є контактори і пускачі, особливістю роботи яких є велика частота комутації (до 1200 комутацій за годину). Їх працездатність та надійність в значній мірі залежать від фізико-механічних властивостей матеріалу контактних деталей. Вибір матеріалу для контактів комутаційних елементів електричних апаратів здійснюється у залежності від виду апарата (вимикачі навантаження, автоматичні вимикачі, контактори, пускачі, апарати кіл керування, реле, тощо), режиму роботи (восьмигодинний, безперервний або тривалий, переривчастий або повторно-короткочасний, а також короткочасний) та категорії його застосування. Контактори, що випускаються в Україні, призначені в основному для категорії застосування АС-3 (прямий пуск асинхронних двигунів з короткозамкненим ротором та відключення працюючого двигуна).

У пускачах і контакторах, зокрема у магнітних пускачах типу ПМЕ, ПМА, ПМЛ застосовують металокерамічні контактні накладки марки КМК-А10м, які містять у своєму складі оксид кадмію (CdO), завдяки якому суттєво збільшується електрична зносостійкість контактів. При цьому слід ураховувати, що оксид кадмію є токсичним, та під дією електричної

дуги, яка виникає в міжконтактному проміжку магнітного пускача в процесі комутації, розкладається на кадмій та кисень й потрапляє до навколишнього середовища.

Державні санітарні правила та норми України (ДСанПіН 2.2.7. 029-99, 2022) відносять кадмій та його сполуки до першого класу токсичних речовин, які небезпечні для здоров'я людини. У цих же правилах зазначається, що оксид кадмію може шкідливо впливати на бронхолегеневу систему, шкіру та підшкірну клітковину, нервову систему, обмін речовин, кровотворну систему та інше.

Також цей матеріал потрапив до переліку матеріалів, не рекомендованих до застосування директивою 2002/95/EU (RoHS directive – Restriction of Hazardous Substances, 2002) Ради Європейського Союзу, яка обмежує застосування небезпечних речовин в новому електричному і електронному устаткуванні, для забезпечення захисту здоров'я людей та навколишнього середовища.

На сесії Ради директорів Програми Організації Об'єднаних Націй з навколишнього середовища, яка регулює використання хімічних речовин, та Глобальному форумі з навколишнього середовища на рівні міністрів був прийнятий стратегічний підхід до міжнародного регулювання хімічних речовин, у тому числі таких, що включають ртуть, свинець і кадмій. У Рішенні заключної доповіді даної сесії (UNEP, UNEA, 2024) зокрема зазначається, що урядам країн потрібно здійснити додаткові заходи для розв'язання проблем і завдань, зумовлених дією свинцю та кадмію.

Таким чином, проблема заміни оксиду кадмію на матеріали, які не є токсичними, безумовно, є актуальною для нашої країни. Ці обставини спонукають до активних досліджень у напрямі пошуку альтернативних КМК-А10 матеріалів.

При виготовленні електричних апаратів приблизно 65 % вартості матеріалів складають контакти на основі срібла. На даний час 25 % світового виробництва срібла витрачається на потреби електроніки й електротехніки, причому 70..80 % його вигорає під дією електричної дуги. Оскільки Україна не має достатніх сировинних ресурсів щодо виробництва цього металу, стає зрозумілою необхідність створення матеріалів, які економлять срібло й одночасно мають належні технічні та екологічні характеристики. Численні дослідження, проведені науковцями у різних країнах, показали можливість застосування в електричних контактах, замість оксиду кадмію, оксидів інших металів, серед яких особливу увагу привертає екологічно безпечний оксид олова.

З огляду на вищесказане, актуальною є задача розробки нових матеріалів для електричних апаратів, які не тільки мають переваги над існуючими серійними зразками щодо

електроерозійної зносостійкості та стабільного низького перехідного опору, але й є екологічно безпечними.

Аналіз застосування контактних матеріалів у низьковольтних електричних апаратах.

Контакти електричного кола можна поділити на такі два типи: контакти комутаційні та контакти ковзання. Комутаційні контакти здійснюють розмикання, замикання чи перемикання складових електричного кола. Контакти ковзання характеризуються поступовим чи обертовим переміщенням робочої поверхні одного елемента по поверхні другого без порушення електричного контакту між ними. Електричні контакти умовно можна поділити на такі групи:

- сильно навантажені;
- середньо навантажені;
- мало навантажені.

Кожний тип потребує певного класу матеріалів із необхідними електричними та контактними властивостями. Проте, незалежно від типу, електроконтактні матеріали повинні мати високі показники тепло- та електропровідності, які можуть коливатися в заданих межах залежно від сфери застосування.

До матеріалів стикових контактів комутаційних апаратів та апаратів керування висуваються такі вимоги (Braunovic M., 2019):

- висока механічна зносостійкість;
- висока електрична зносостійкість;
- висока стійкість до зварювання;
- висока електропровідність;
- висока теплопровідність;
- низький та стабільний перехідний опір;
- низька схильність до взаємодії з хімічно активними складовими атмосфери – двоокисом вуглецю, сірководнем, двоокисом сірки, аміаком, киснем тощо;
- забезпечення надійного кріплення до контактотримача зварюванням, паянням чи заклепуванням;
- низька вартість при заданому рівні надійності.

Перераховані вимоги не може задовольнити жодний із чистих металів. Зокрема, мідь, яку можна було б уважати ідеальним контактним матеріалом (питома маса γ = 8,96 г/см^3; питомий опір ρ = 0,017 мкОм·м; питома теплопровідність λ = 406 Вт/(м·К); питома теплоємність – 386 Дж/(кг·К); температура топлення – 1083 °С; температура кипіння – 2600

°C; твердість Нв = 35 кгс/мм^2; межа міцності при розтягуванні 14 кгс/мм^2), якби не схильність до окислення, унаслідок чого на поверхні утворюються плівки з надзвичайно високим опором, що збільшує перехідний опір контактів, а відтак сприяє неприпустимому перегріванню або навіть порушенню контакту. Тому в сучасній апаратурі мідні контакти замінюються композиційними на основі міді. Однак, мідь має широке застосування в комутаційних апаратах з ручним керуванням, які працюють зі значними механічними зусиллями і з ковзанням робочих поверхонь.

Благородні метали (золото, платина, паладій тощо), тобто метали з низькою хімічною активністю у недавньому минулому мали широке застосування в контактах електричних реле, а також як захисне покриття в контактах електричних з'єднувачів (золото), які використовувалися в слабкострумовій апаратурі, призначеній переважно для військово-промислового комплексу.

Суттєво меншу хімічну активність порівняно з міддю має срібло, тому перехідний опір контактів, виготовлених зі срібла, є відносно стабільним. Слід зазначити, що чисте срібло у контактних матеріалах застосовується досить рідко, але срібло застосовується в контактах як домінуючий компонент у композиціях з іншими металами та їх сполуками. Чисте срібло має ряд недоліків і найсуттєвіші з них такі (Hertel W., Schedler D., 2022):

- низька міцність;
- схильність зварюватися при комутації електричного струму;
- схильність до злипання при високому контактному тиску;
- схильність до направленого переносу матеріалу при комутації постійного струму;
- схильність до сульфідної корозії, особливо при одночасному впливові вологи та високої температури;
- схильність до "розтікання" при дотику з ізоляційними матеріалами під дією електричного потенціалу у вологому середовищі, що може викликати коротке замикання, особливо в перемикачах.

З метою усунення вказаних недоліків до контактного матеріалу на основі срібла вводять домішки різних сполук. Перспективними матеріалами для контактів потужних повітряних вимикачів є сполуки на основі срібла з домішками вольфраму (W-Ag) та молібдену (Mo-Ag), а для контактів оливних вимикачів подібні матеріали на основі міді W-Cu та Mo-Cu. У роботі (Braunovic M., Myshkin N.K., 2019) констатується факт, що ерозійна стійкість композиційних матеріалів Fe-Cu, Fe-Cu-Sb, W-Cu-Sb-Fe, W-Fe-Cu та інших при розряді у вакуумі виявляється на порядок вища, ніж у міді. Тому вони широко застосовуються у вакуумних вимикачах.

Для середньо навантажених контактів використовуються матеріали на основі срібла й оксидів, срібла і нікелю, срібла, нікелю та графіту.

З метою запобігання окисленню металів групи заліза, тугоплавких металів та їхніх сполук (боридів, нітридів та ін.) до складу електроконтактного матеріалу вводять графіт, який під дією електричної дуги перетворюється на газ, що сприяє відновленню електроконтактного матеріалу та запобігає його окисленню. Оптимальна кількість графіту для цього випадку становить 3–7 % від маси контактного матеріалу. У роботі (Buldum A., 2021) наведено дані про те, що введення в срібну матрицю графіту близько 3 % від маси сприяє зміцненню контактів.

У роботі (Johler W., 2020) обґрунтовується оптимальний вміст графіту в мідних розмикаючих контактах, який, як правило, не повинен перевищувати 5 % від маси контактного матеріалу. Композиції з більшим вмістом графіту можна застосовувати для рухомих контактів (наприклад, електрощітки електричних машин). Введення до срібла графіту більш ніж 10 % погіршує технологічні властивості композиції, а при великому числі комутацій може викликати погіршення ізоляційних властивостей апарата.

Відомо, що якість контактів значною мірою залежить від структури графіту. Так, застосування графіту із лускоподібною структурою погіршує якість дугостійких контактів, оскільки призводить до збільшення електричного опору в напрямку проходження струму.

Чисте срібло, краще кажучи, стопи срібла з малим вмістом домішок застосовуються в біметалевих контактах електромеханічних реле. Як робочий шар у таких контактах найчастіше застосовуються стопи Ср999, СрМ-0,2 та СрН-0,1.

Стоп Ср999 – це майже чисте срібло з незначним вмістом домішок (табл. 1).

Таблиця 1

Хімічний склад срібного стопу Ср999

Марка	Хімічний склад , %						
	Срібло, не менше %	Домішки, не більше					
		Свинець	Залізо	Сурма	Вісмут	Мідь	Усього
Ср999	99,90	0,004	0,035	0,003	0,003	0,055	0,10

Контактні матеріали Ср999 застосовуються в електромагнітних реле типу ПЕ-40, ПЕ-41, ПЕ-43 та інших з номінальним струмом до 5 А.

Свинець при топленні розчиняється в сріблі та при внутрішньому окисленні подрібнює зерна срібної матриці.

Залізо не розчиняється в срібній матриці, а підвищує твердість стопу (твердість заліза Нв = 45 кгс/мм^2) і температуру топлення (температура топлення заліза 1539 °С), що в цілому підвищує електроерозійну стійкість контактів.

Сурма підвищує твердість стопу, оскільки створюються тверді розчини сурми на основі срібла.

Вісмут є сильним окислювачем і при розчинності його в сріблі, залізі, міді та при внутрішньому окисленні створюються оксиди елементів, які утворюють дрібнодисперсну структуру срібної матриці й підвищують її твердість до 80 кгс/мм^2.

При внутрішньому окисленні стопу срібло-мідь збільшується зносостійкість і опір контактів зварюванню та обгоранню.

Введення вищеперерахованих домішок до стопу срібла і його внутрішнє окислення дозволило підвищити електроерозійну стійкість у 4 рази порівняно із чистим сріблом (Hartmann U., 2010).

Контактні матеріали типу СрМ-0,2 застосовуються в біметалевих контактах реле РПЛ і магнітних пускачах серії ПМЛ з номінальним струмом 10–16 А і ступенем захисту IP54 (табл. 2).

Таблиця 2

Хімічний склад срібного стопу типу СрМ-0,2

Марка	Хімічний склад , %					
	Срібло, не менше %	Домішки, не більше				
		Мідь	Нікель	Бор	Ітрій	Усього
СрМ-0,2	99,196	0,5	0,2	0,1	0,004	0,804

Домішка нікелю 0,2 % маси вповільнює зростання зерна срібла. Вплив нікелю на подрібнення зерна срібла обґрунтовано тим, що в рідкому сріблі розчиняється 0,16 % його маси, а в твердому сріблі при температурі 400 °С – 0,012 % маси нікелю. Таким чином, при затвердінні срібла з розчиненим 0,16 % маси нікелю виділяються його дрібні частинки, які збільшують центри кристалізації.

Введення міді створює стоп твердого розчину, що підвищує його твердість.

При температурі 600 °С ітрій розчиняється в сріблі, після внутрішнього окислення твердість стопу складає Нв = 110 кгс/мм^2, унаслідок чого підвищується електроерозійна стійкість.

Бор у з’єднаннях з інгредієнтами сплаву при внутрішньому окисленні проявляє значний ступінь окислення. При цьому створюється дрібнозерниста структура і підвищується електроерозійна стійкість.

Контактні матеріали типу СрН-0,1 застосовуються в контактах теплових реле РПЛ і магнітних пускачах, що комутують струм до 10 А (табл. 3).

Таблиця 3

Хімічний склад срібного стопу типу СрН-0,1

Марка	Хімічний склад , %					
	Срібло, не менше %	Домішки, не більше				
		Мідь	Нікель	Фосфор	Берилій	Усього
СрН-0,1	99,768	0,12	0,1	0,003	0,009	0,232

При комутації струму срібло на робочій поверхні контакту плавиться і поглинає кисень з повітря, який бурхливо виділяється при застиганні срібла, і його розбризкує. Мідь усуває даний ефект за рахунок поглинання кисню з розплавленого срібла і зменшує його розбризкування, що підвищує електроерозійну стійкість контактів.

Мідь зі сріблом утворюють твердий розчин і підвищують його міцність.

Введення нікелю подрібнює зерна срібла і структура стопу стає дрібнозернистою, а це підвищує міцність і твердість. Для розкислення стопу вводять фосфор, після чого злитки прокатують і виготовляють контакти необхідної форми.

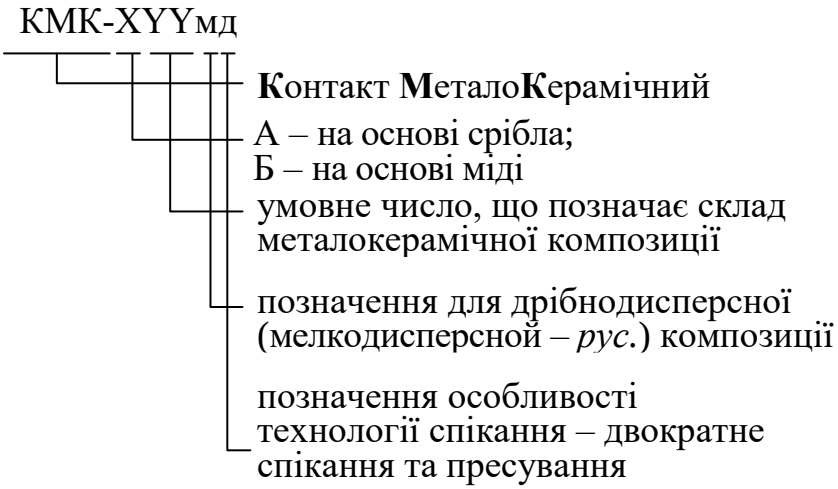
Срібні стопи СрМ-0,2 та СрН-0,1 є малолегованими, вони містять до 1 % (за масою) легуючих компонентів, які надають стопам необхідних властивостей щодо комутації струмів низького і середнього рівнів: високу електропровідність, міцність і стійкість до зварювання.

Застосування методів порошкової металургії дозволяє створити так звані металокерамічні контакти (МК), які певною мірою задовольняють більшість суперечливих вимог до стикових контактів комутаційних апаратів та апаратів керування.

Металокерамічними називають контакти, виготовлені методом твердофазного спікання суміші порошків різних металів та окисів, підібраних у певних пропорціях.

Основними перевагами металокерамічних контактів перед контактами, виготовленими із чистих металів та стопів, є майже повна безвідходність та можливість отримувати властивості контактних матеріалів, які непритаманні чистим металам та стопам.

Ефективність застосування металокерамічних контактів виявилася настільки значною, що був створений державний стандарт, який регламентував основні різновиди й склад металокерамічних контактів (ДСТУ 2848-94, 1996). За цим стандартом металокерамічні контакти мали позначатися так:



Сферою дії стандарту були контакт-деталі, які містять срібло з підшаром і без підшару та виготовлені методом твердофазного спікання для замикання й розмикання електричних кіл у комутаційних апаратах напругою до 1000 В. Цей стандарт передбачав випуск підприємствами композиції, марки яких наведено в табл. 4.

Серед найбільш розповсюджених металокерамічних композицій слід зазначити такі:

– А00 – чисте срібло (не менше 99,9 %), якщо контакт виготовлено за технологією МК;

– А10 – 85,0±05 % срібла, решта – окис кадмію (у ГОСТ 19725 наводиться лише позначення для дрібнодисперсної композиції – А10м), стара назва – СОК15;

– А30 – 70,0±05 % срібла, решта – нікель, стара назва – СН30; (у ГОСТ 19725-74 наводиться також позначення для дрібнодисперсної композиції – А30м, а також А30мд – для композиції, яка передбачає подвійне спікання).

Таблиця 4

Склад металокерамічних композицій

Марка контакту	Масова частка матеріалу, %						
	Срібло	Оксид кадмію	Оксид міді	Нікель	Графіт	Кадмій	Залізо
КМК-А00	99,9	–	–	–	–	–	–
КМК-А10м	85+/-0,5	решта	–	–	–	–	–
КМК-А20м	90+/-0,5	–	решта	–	–	–	–
КМК-А30	70+/-0,5	–	–	решта	–	–	–
КМК-А30м	70+/-0,5	–	–	решта	–	–	–
КМК-А30мд	70+/-0,5	–	–	решта	–	–	–
КМК-А31	60+/-0,5	–	–	решта	–	–	–
КМК-А31м	60+/-0,5	–	–	решта	–	–	–
КМК-А33мд	69+/-0,5	–	–	29	2+/-0,3	–	–
КМК-А40	95+/-0,5	–	–	–	решта	–	–
КМК-А41	97+/-0,5	–	–	–	решта	–	–
КМК-А50	76+/-0,5	–	–	0,8+/-0,1	–	решта	0,4+/-0,1
КМК-А32	68+/-0,5	–	–	29	3+/-0,3	–	–

Контакт марки КМК-А30 має високу електроерозійну стійкість порівняно зі сріблом і низький стабільний перехідний опір. Дрібнодисперсний контактний матеріал з розміром частинок 1 мкм (КМК-А30м) має електроерозійну стійкість у 1,5..2 рази вищу, ніж матеріал із частинками 10..100 мкм (КМК-А30).

Стабільність перехідного опору контактів КМК-А30 пояснюється властивостями поверхневих плівок, що утворюються на робочих поверхнях контактів. Нікель, окислюючись на повітрі під дією електричної дуги, утворює оксиди різного складу, які не сплавляються між собою та утворюють різнорідні тонкі плівки (Lindmayer M., Bohm W., 2010).

Основний недолік контактів марки КМК-А30 – низька стійкість до зварювання при комутації струму. Для збільшення стійкості до зварювання при перевантаженнях та струмах короткого замикання контакти марок КМК-А30м використовують у парі з контактами КМК-А41.

Контакти КМК-А41 мають високу стійкість до зварювання при перевантаженнях та струмах короткого замикання, низький і стабільний перехідний опір. Недолік матеріалу – низькі твердість і міцність, які знижують електроерозійну стійкість. Тому композиції марки КМК-А41 на нерухомих контактах застосовують у парі з контактами КМК-А30 на рухомих контактах, наприклад, у вимикачах з робочими струмами до 160 А.

У вимикачах з більшими робочими струмами композиція КМК-А41 не забезпечує необхідну електроерозійну стійкість, тому в таких апаратах для нерухомих контактів застосовують інші композиції. Зокрема, у вимикачах А3700 для нерухомих контактів застосовується композиція марки КМК-А33м, а на рухомих контактах – КМК-А30м.

Як матеріал нерухомого контакту в деяких вимикачах застосовується металокерамічна композиція КМК-А33мд, яка містить 69 % срібла, 29 % нікелю та 2 % графіту, який підвищує дугостійкість та зменшує схильність контактів до зварювання.

У деяких магнітних пускачах на струми 10 та 16 А відкритого виконання (ступінь захисту IP00) наразі застосовують контакти марки СрН10. Цей композиційний матеріал контактів містить 90 % (за масою) срібла та 10 % нікелю. Цей матеріал має низький і стабільний перехідний контактний опір, а також відносно високу (хоча й меншу, ніж у КМК-А10м) електроерозійну стійкість.

Низький перехідний опір забезпечується тим, що хоча при нагріванні до 500 °С нікель й окиснюється, але окисна плівка виявляється тонкою і слабко утримується на робочій поверхні контакту, до того ж при навіть незначній механічній дії руйнується (ТУ 16-685.026-96).

У матеріалі контакту СрН10 срібло і нікель майже не змішуються між собою ані в твердому, ані в рідкому стані, а незначний відсоток нікелю, який усе ж таки розчиняється в сріблі, дає можливість отримати дрібнозернисту структуру срібла, яка значно підвищує електроерозійну стійкість контактів і знижує їх схильність до зварювання.

Донедавна в контакторах та пускачах широко застосовувалися однорідні контакти марки КМК-А10 (85 % срібла та 15 % оксиду кадмію), яка має унікальну дугогасну здатність, стабільність контактного опору, а також відносно високу стійкість до ерозії та зварювання.

Високі дугогасні властивості цієї композиції зумовлені низькою температурою сублімації CdO, яка становить 900 °С, і є нижчою температури топлення срібла – 960,5 °С. Стабільність контактного опору забезпечується низькою термічною стійкістю CdO, у результаті контактні поверхні виявляються вільними від накопичень оксидів.

Інтенсивний розпад CdO відбувається при температурі вище 1000 °С з виділенням значного об'єму газоподібного кисню і парів кадмію – об'єм газоподібного кисню і парів кадмію перевищує об'єм твердого CdO приблизно у 10 000 разів. Таке бурхливе виділення кисню та кадмію механічно видуває дугу, примушуючи її переміщуватися по робочій поверхні контактів. У той же час дуга горить в атмосфері парів кадмію і кисню, потенціал іонізації яких вищий, ніж парів срібла (потенціал іонізації атомів срібла становить 7,54 В, кадмію – 8,96 В, кисню – 13,55 В), унаслідок чого дуга в середовищі продуктів дисоціації CdO гасне швидше, ніж у парах срібла.

Унаслідок дуже швидкого пересування дуги по робочих поверхнях мікроструктура основної маси контактів не змінюється і тим самим забезпечується їх термічна стійкість.

Окис CdO, який утворюється внаслідок зворотної реакції окиснення парів кадмію в області більш низьких температур при гасінні дуги, осідає на робочій поверхні контактів, перешкоджаючи їх зварюванню при замиканні.

До останнього часу, ураховуючи свої унікальні контактні властивості, композиція Ag-CdO залишалась неперевершеною. Але екологічні вимоги роблять більш актуальним пошук альтернативних композицій. При дослідженнях і експлуатації апаратів відбувається ерозійне зношування контактів з утворенням небезпечного газу, який виділяється і шкідливо впливає на організм людини (ДСанПіН 2.2.7. 029-99, 2022). Тому за останні роки були зроблені спроби заміни CdO іншими оксидами металів. В основному такі дослідження проводяться в лабораторіях таких країн, як Німеччина (фірма «Додуко»), Японія, Китай (технічний університет м. Ксикань), США, Україна (ІПМ НАНУ), і вони показали, що ефективним замінником оксиду кадмію може бути оксид олова SnO_2 (за класифікацією щодо ступеня впливу на організм людини оксид кадмію належить до речовин І класу небезпеки, а оксид

олова – до III (ДСанПіН 2.2.7. 029-99, 2022), або ще ZnO, CuO, PbO. До складу таких композицій деякі автори рекомендують додавати незначні домішки оксидів вісмуту Bi_2O_3, індію In_2O_3. Автори (Lima Antonio E. Shen Yuan, 2019) розробили біметалевий контактний матеріал з робочим шаром із композиції Ag-SnO_2 (10–12 мас. %) і технологічним прошарком з міді та мідно-нікелевої композиції. Але відомо, що основним недоліком КМ на основі Ag-SnO_2 є високий контактний опір, що може призводити до перегрівання при довготривалих навантаженнях, особливо при незначних величинах контактного натиску.

Технологія виготовлення спечених електричних контактів.

При створенні електроконтактного матеріалу, який працює в режимі тертя або комутації електричного струму, необхідно науково обґрунтувати вибір компонентів матеріалу, їхнє оптимальне співвідношення та умови виготовлення шихти, спосіб термомеханічної обробки тощо.

Виходячи з огляду науково-дослідних робіт і аналізу технічних періодичних видань, на сьогодні ще існують варіанти підвищення експлуатаційних службових властивостей КМ за рахунок застосування традиційних технологічних методів порошкової металургії, яка передбачає оптимізацію складу композиційних КМ, а також за рахунок застосування новітніх сучасних технологічних методів виготовлення КМ, які можуть дозволити отримувати матеріали з дрібнозернистою структурою з розміром зерна 0,1-..1,0 мкм, тобто:

- одинарним пресуванням порошкових сумішей з наступним спіканням, допресуванням і відпалюваням (КМК-10мд, застосуванням високотехнологічного субтрактивного срібного порошку для контактів Ср 0712;
- спільним прокатуванням заготовок сплавів з наступним дифузним внутрішнім окисленням і вирубуванням контактів зі штабу; прокатуванням порошків із проміжними термообробками і наступним вирубуванням контактів зі штабу;
- екструзією і докатуванням;
- екструзією і прокатуванням порошкових заготовок з наступним вирубуванням контактів зі штабів (цей метод уважається найбільш універсальним, оскільки дозволяє отримувати контакти зі різноманітних срібловмісних композиційних матеріалів, при цьому забезпечується вища ерозійна стійкість і міцність з'єднання шарів; контакти КМК ПА-09; -12; -13);
- застосуванням технології IRE (Indirect Repeat Extrusion), яка дозволяє виготовлювати волокнисті композиційні матеріали, у яких волокна розміщені перпендикулярно до поверхні контакту; за рахунок цього досягається велика економія срібла шляхом уведення більшого відсотка домішок до матриці (Muller K., Stockei D., 2015).
- застосуванням технології високошвидкісного електронно-променевого випаровування

металів і неметалів і наступної конденсації парового потоку на підкладку для отримання високодисперсних матеріалів (контакти МДК-1; -2; -3).

В окремих випадках використовуються методи високотемпературного імпульсного або статичного чи ізостатичного пресування. Використання сил міжмолекулярного зчеплення на стадії пресування порошків, явищ в'язкої текучості та капілярних ефектів (поверхневих сил, змочування, капілярного тиску) і дифузії на стадії твердофазового або рідкого спікання і просочення дозволяє об'єднати в одному матеріалі різні фазові складові широкого кола речовин. Вибір початкової структури порошків та армуючих елементів і відповідної технології дозволяє забезпечити необхідну структуру матеріалу за дисперсністю та розподілом фазових складових із необхідними електроконтактними властивостями.

Кожний клас електроконтактних матеріалів (високовольтні, низьковольтні, контакти для середньо й слабо навантажених апаратів) виготовляють за певними технологічними схемами. Оптимальним технологічним варіантом виготовлення контактів для високо- і низьковольтних апаратів є метод просочення спеченого пористого тугоплавкого каркасу.

Загальною вимогою при синтезі електроконтактного матеріалу є наступне: він повинен являти собою псевдосплав, який складається з тугоплавкої твердої жароміцної та дугогасної компоненти, що утворює просторовий каркас-матрицю, і відносно легкоплавкої, електропровідної та теплопровідної компоненти, яка слугує наповнювачем матриці.

Першою умовою надійності роботи такого псевдосплавного матеріалу є його монолітність (відсутність пористості та висока міцність адгезійного зв'язку). Це забезпечується відповідними технологічними умовами виготовлення – уведенням домішок, які сприяють зниженню крайового кута змочування, підвищенню капілярного тиску й міцності адгезійного зв'язку. Тонкодисперсні інертні наповнювачі обмежують спікання поверхневих шарів пористої тугоплавкої заготовки, покращують доступ просочуючого розплаву і його рівномірне розтікання по каналах пор у матеріалі заготовки.

Оптимальна для цього псевдосплаву буде мікроструктура, яка утворена рівномірним по всьому об'єму контакту безперервним каркасом із тугоплавкої складової в матриці з легкоплавкого компоненту або сплаву. Легкоплавкими компонентами зазвичай слугують мідь, срібло та їх сплави.

Контактні деталі із псевдосплаву на основі вольфраму, молібдену, карбіду вольфраму або карбіду молібдену для забезпечення приварки або пайки повинні мати підшар із міді або срібла. Для покращання тепловідведення від робочої поверхні слугує шар лугостійкого псевдосплаву завтовшки 4..5 мм. Така комбінована деталь має майже в 5 разів більший термін служби, ніж виготовлена лише з порошкового псевдосплаву.

Для низьковольтної апаратури найчастіше використовують матеріали на основі срібла або міді з домішками оксидів (CdO, ZnO, SnO, MgO, NiO та ін.). Оптимальною мікроструктурою у цьому випадку є рівномірний розподіл у матриці компонентів, які додані у вигляді окремих вкраплень або ланцюжків, що відіграють роль дисперсно-керуючих домішок і в той же час виступають у ролі теплопоглинальних складових у процесі термічного розкладу. Виготовляються такі матеріали твердофазним спіканням пресованих із суміші порошків компонентів із подальшою деформацією.

Змінюючи технологію виробництва, можна отримати контакти з різною мікроструктурою. Розміри включень оксиду металу змінюються від десятих часток до 30..50 мкм. Дисперсні структури можна одержати використовуючи твердофазне спікання пресовок із суміші порошків, які утворюються спільним осадом з подальшою деформацією або відливкою сплаву срібло-метал з подальшим внутрішнім окисненням металу .

Електричні контакти з високою дисперсністю менш пластичні, вони мають суттєві переваги за електроерозійною стійкістю перед литими й спеченими контактами більш крупнозернистої будови.

Технологія виготовлення слабкострумових контактів складається із пресування заготовок сумішей певного складу та спікання. Після цього заготовки піддаються механічній деформації (прокатка, волочіння). Ефективним шляхом усунення залишкової пористості є холодне й гаряче екструдування, гаряче та ізостатичне пресування. Мікроструктура таких матеріалів є електропровідною та теплопровідною матрицею, у якій рівномірно розподілені домішки.

Остання операція механічної обробки тиском забезпечує створення анізотропної структури псевдосплаву, отримання волокнистої будови з виходом волокон мікрофаз до робочої поверхні контакту. Це суттєво впливає на режим роботи контактів та їхню електропровідність, ерозійну і механічну стійкість.

З отриманого прокату (дроту або стрічки) шляхом штамповки й висадки можна виготовити контакти довільної форми та розмірів. У деяких випадках висадку контактів із дроту проводять одночасно з їхнім кріпленням до контактотримача.

Проведений аналіз дав підстави стверджувати, що розв’язання проблеми підвищення екологічної безпеки та електроерозійної стійкості контактних матеріалів можливе на основі науково-технічних передумов вибору екологічно чистих оксидних та туготопних інгредієнтів, дослідження їх фізико-хімічних властивостей взаємодії між собою та металевою матрицею.

Обґрунтування методів створення екологічно безпечних та ерозієстійких композиційних контактних матеріалів.

Комутуючі пристрої магнітних пускачів під час експлуатації зазнають впливу численних факторів, які призводять до таких руйнувань:

- механічний знос;
- дугова електрична ерозія;
- місткова електрична ерозія;
- корозія під впливом навколишнього середовища;
- дугова корозія;
- теплове зварювання.

Відповідно до різновидності зносу контактів постає питання перед контактним матеріалом (КМ) щодо експлуатаційних вимог, залежно від того, який вид руйнування переважає в даних конкретних умовах експлуатації.

При механічному зношуванні контакти стираються, розтріскуються, деформуються і нагріваються під дією кінетичної енергії при їх замиканні. У цьому випадку КМ повинен мати високі механічні властивості: твердість, граничну міцність при ударі, тиску і зсуві, помірний модуль пружності та пластичність, низький коефіцієнт тертя.

Контакти, які працюють при номінальних струмах 40-100 А, зазнають руйнування та ерозії в результаті впливу електричної дуги. При цьому для зменшення ерозії матеріал контактів повинен мати наступні властивості: високу температуру плавлення і кипіння, електро- і теплопровідність, критичне значення напруги і струму для створення дуги, твердість, низьку пружність парів металу при температурі дуги, мати високий поверхневий натяг та кут змочування металу в рідкому стані наближений до нуля, мікродисперсну структуру композиції.

Корозія робочих поверхонь контактів пускачів, яка відбувається під дією хімічноактивних домішок середовища, також є одним із головних факторів зносу і відмов, тому основні властивості для зменшення цього впливу є такі:

- високий електродний потенціал матеріалу;
- низька хімічна спорідненість матеріалу до кисню, азоту, вуглецю;
- низька термічна стійкість ізоляційних плівок;
- висока пружність дисоціації продуктів корозії при температурі електричної дуги;
- низька електрична та механічна міцність ізоляційних плівок;
- структура плівок.

На частоту і силу зварювання впливають такі властивості контактних матеріалів:

- температура плавлення;
- електро- і теплопровідність;

- твердість;
- властивість до окиснення робочих поверхонь контактів;
- мікроструктура матеріалу.

Складні умови експлуатації контактів та чисельні фактори – електричні, механічні та хімічні, які впливають на роботу контактів, затрудняють вибір контактного матеріалу.

Рід і величина струму, напруга, характер навантаження – омічний, індуктивний, ємнісний, контактний тиск, контактний розхил, швидкість і частота ввімкнень, склад, вологість і температура середовища, у якому знаходяться контакти, та багато інших факторів впливають на поведінку контактів в експлуатації.

Один і той же матеріал, стійкий до зносу за одних умов, при зміні одного із факторів може виявитися зовсім непридатним для роботи.

У загальному вигляді контакти повинні характеризуватися наступними фізичними параметрами:

- стабільністю контактного перехідного опору;
- високою питомою електропровідністю;
- високою ерозійною стійкістю та корозійною тривкістю;
- високою дугостійкістю і стійкістю до зварювання;
- поєднанням механічної міцності та високої пластичності.

Практично неможливо підібрати універсальний матеріал, який би відповідав усім названим вимогам, тому залежно від функціонального призначення контактного вузла доводиться приймати компромісне рішення. Контакти пускачів, які працюють в області малих та середніх струмів, повинні, перш за все, забезпечувати стабільність перехідного опору в поєднанні з високими дугостійкістю та стійкістю до зварювання (ДСТУ 2846-94).

Перехідний опір залежить від фактичної площі дотику контактів і від питомого опору контактного матеріалу. Ефективна площа контактування залежить від величини контактного натиску і з його ростом збільшується за експоненціальною залежністю до того часу, поки напруга стискання не буде вищою за межу текучості матеріалу. З іншого боку, перехідний опір залежить від опору граничного шару, який визначається його складом (наявність оксидних, сульфідних та інших плівок, пилу тощо) і питомим електричним опором.

Ураховуючи експлуатаційні та екологічні вимоги до комутуючих пристроїв пускачів, та з метою економії благородних металів розробки КМ доцільно проводити в напрямі покращення властивостей багатокомпонентних композиційних КМ на основі срібла і тугоплавких сполук.

У кожному окремому випадку при виборі матеріалу для контактів необхідно керуватися деякими загальними положеннями, головні з них наведено нижче.

До головних факторів, які обумовлюють вибір матеріалів контактів, на думку автора, відносяться наведені нижче:

1. Параметри комутуючого кола:

а) величина номінального струму. Чим більша величина номінального струму, тим сильніше нагрівання контактів. Перевагу мають метали з високою тепло- і електропровідністю, які не окиснюються при малому контактному натиску;

б) рід струму. Електрична ерозія контактів більш виражена при постійному струмі. При змінному струмі перенос матеріалу зменшується, але більше піддається ерозії контакт, температура якого вища. Збільшується оплавлення та обгоряння КМ;

в) комутуючий струм. При струмі нижче за граничний, електрична дуга не виникає. При збільшенні струму вище за граничний (коли з'являється дуга), явища ерозії, зварювання, окиснення та обгоряння зростають разом з енергією дуги і струмом;

г) напруга між контактами. Вона визначає виникнення контактної дуги. Нижче граничного значення (для кожного КМ – своє значення) – дуга не виникає, вище – з'являється контактна дуга;

д) характер навантаження. Залежно від характеру навантаження змінюються пускові струми, які комутують пускачі, а також від значення $\cos\varphi$ змінюється індуктивність кола. Це призводить до виникнення перенапруг і до збільшення часу горіння дуги та ерозії при комутації, а також сприяє зварюванню контактів;

е) наявність чи відсутність дугогасильних пристроїв;

ж) частота і загальна кількість комутаційних циклів прямо пропорційно впливають на інтенсивність і величину ерозії контактів. Завищена частота спричиняє перегрівання контактів вище за допустиму температуру.

2. Параметри комутуючих пристроїв пускача:

а) номінальний контактний натиск. Незначний натиск зменшує ерозію матеріалу, але спричиняє підвищення перехідного контактного опору. При достатньо великих зусиллях можна застосовувати матеріали, які окислюються, зважаючи при цьому на характеристики механічної міцності;

б) конструктивні фактори. Деренчання контактів при замиканні значно збільшує ерозію і зварювання внаслідок послідовних комутаційних операцій пускового струму;

в) швидкість контактів при комутації. Збільшення швидкості при розмиканні скорочує час горіння дуги при постійному струмі, зменшуючи ерозію. Велика швидкість при змінному струмі збільшує перенапругу і час горіння;

г) розміри та геометрична форма контакт-деталей. Розміри (діаметр, товщина) потрібно стандартизувати, узгоджуючи з величиною пускача та виходячи з економічної доцільності. Геометричну форму вибираємо, виходячи зі збільшення умовної площі контактування і зменшення ерозії матеріалу;

д) величина розхилу контактів має значення, оскільки вона визначає максимальну напругу на контактах, яка не здатна пробити цей контактний проміжок;

е) теплофізичні та механічні характеристики КМ для розривних контактів (стійкість проти електричної ерозії, зварювання; корозійна тривкість; достатній опір механічному зношуванню, технологічність; низька вартість і не дефіцитність).

3. Кліматичний вплив навколишнього середовища викликає ріст «хімічних плівок» на контактних поверхнях, що призводить до збільшення перехідного опору та поступових відмов пускача.

Фізичні, теплові, механічні та хімічні властивості контактних матеріалів, які обумовлюють зносостійкість контактів, наведено в табл. 5.

Немає можливості безпомилково рекомендувати матеріал, придатний для роботи в будь-яких заданих умовах, необхідно кінцевий вибір обґрунтовувати на випробуванні в контактних апаратах і в умовах, що відповідають дійсним умовам роботи контактів в експлуатації (ДСТУ 2993-95).

Таблиця 5

Властивості матеріалів, які впливають на зносостійкість контактів

№	Групи властивостей матеріалу	Характеристика властивостей
1	Механічні	Твердість, границя міцності при тиску і зсуву, пластичність, модуль пружності коефіцієнт тертя
2	Електрофізичні	Електропровідність, теплопровідність, струм і напруга утворення дуги, робота виходу електрона з кристалічної решітка та потенціал іонізації атому металу при випаровуванні, величина коефіцієнта Томсона, кут змочування металу в рідкому стані та його поверхневий натяг, атомний об’єм матеріалу, термоелектрорушійна сила

3	Теплові	Температура рекристалізації, кипіння, плавлення, сублімації. Теплота плавлення, кипіння, сублімації, теплоємність. Пружність парів металу при температурі дуги
4	Електрохімічні	Величина електродного потенціалу, хімічна спорідненість з киснем, азотои, сіркою. Механічна та електрична міцність ізоляційних плівок. Пружність дисоціації продуктів корозії
5	Структурні	Тип кристалічної решітки, мікроструктура в композиційних матеріалах, види сплавів. Орієнтування кристалів згідно з напрямком теплового та електричного потоків

Однак при сучасних знаннях природи зносу розривних контактів можна дати основні вказівки щодо вибору типу матеріалу залежно від потужності, при якій призначено працювати контактам.

Для малонавантажених контактів, що працюють нижче межі дугоутворення і піддаються містковій ерозії, найбільш придатні метали з високою тепло- і електропровідністю. Допустиме слабе легування іншими металами, в тому числі і не благородними, з метою підвищення твердості і зменшення голкоутворення.

Для середньонавантажених контактів, які працюють з утворенням контактної дуги, придатні тугоплавкі метали, а також сплави типу твердих розчинів. Для зменшення зварювання доцільно вводити в сплав оксиди металів, які при певних умовах дисоціюють, не порушуючи контактної провідності.

Для високонавантажених контактів найбільш придатні композиції, які поєднують високу зносостійкість тугоплавких металів та електро- і теплопровідність, наприклад, Cu чи Ag .

Принципи вибору інгредієнтів композиційного контактного матеріалу.

При виборі інгредієнтів композиційного матеріалу необхідно враховувати протидію їх електричній ерозії, зварюванню, збільшенню перехідного опору при комутації струму.

Найбільше застосування в магнітних пускачах мають контактні матеріали матричної будови, що являють собою електропровідну і теплопровідну матрицю зі срібла, і рівномірно розподіленими в ній домішками (інгредієнтами) з відмінними фізико-механічними властивостями.

За видом інгредієнтів композиційні матеріали матричної будови можна класифікувати на три основні групи:

- матеріали з неметалевими інгредієнтами (оксиди, карбіди, нітриди);
- матеріали з металевими інгредієнтами;
- матеріали, що включають інгредієнти металеві й неметалеві.

Зазначені інгредієнти виконують різні функції в матеріалі: зміцнюють матрицю, спричиняють гасіння електричної дуги, впливають на роботу виходу електрона тощо.

На основі привила прив'язок у матеріалах матричної будови електрична дуга закріплюється на найменш тепло- і електропровідних фазах, які в гетерогенних композиціях на основі срібла відповідають частинкам (інгредієнтам), що наповнюють матрицю. Ці частинки, які сприймають теплове навантаження, розігріваються до температури випаровування і постачають масу матеріалу в міжконтактний проміжок. Матрична фаза, що знаходиться з боку від стовпа дуги, інтенсивно відводить тепло від зони термічної дії дуги. До виробки розподілених у них частинок матриця залишається в твердому агрегатному стані та не постачає масу в міжконтактний проміжок. Зі зносом частинок електрична дуга переходить на матрицю, розігріває її та починається випаровування маси контактного матеріалу із матричної фази.

Таким чином, рухаючись за поверхнею контактів електрична дуга послідовно руйнує як частинки, так і матрицю. У зв'язку з тим, що теплопровідна маса інтенсифікує відведення тепла від інгредієнтів, на яких закріплена дуга (що знижує розігрівання), ерозійна стійкість гетерогенної композиції може перевищувати ерозійну стійкість як матричної, так і наповнюючої фази, якщо взяти їх окремо.

Основними критеріями при виборі інгредієнтів є їх висока термодинамічна стабільність, яка характеризується відсутністю хімічної взаємодії з сріблом і малою схильністю до коалесценції за розчинно-осадовим механізмом при високих температурах. У першу чергу, цим вимогам відповідають термодинамічні стійкі тугоплавкі з'єднання, такі як оксиди MoO_3, Cr_2O_3, WO_3.

У срібній матриці оксиди підвищують міцність, границю текучості, твердість і температуру рекристалізації. Вони також можуть викликати дугогасильний ефект, що перешкоджає зварюванню контактів при комутації струму.

Структурні зміни на поверхнях при комутації струму, обумовлюють зносостійкість контактної пари та її функціональну надійність. Дослідження закономірностей структурних перетворень на робочих поверхнях визначає можливість створення оптимальної вихідної структури і комплексу фізико-механічних властивостей контактного матеріалу.

Розробка електроерозійних контакт-деталей на основі срібла неможлива без урахування закономірностей і механізму масопереносу матеріалу контакт-деталей уу процесі комутації струму електричного кола.

Принципи створення ерозієстійких розривних контакт-деталей передбачають наявність у срібній струмопровідній матриці зміцнювальних домішок з відмінними від срібла теплофізичними і механічними властивостями.

Введення до складу контактних композицій на основі срібла дисперсних фаз, що не взаємодіють з останнім, а також легування срібла тугоплавкими металами дозволяє створити гетерофазну структуру, яка забезпечує рухомість основи дуги, що зменшує ймовірність утворення розплавленого кратера і значно знижує видалення матеріалу з робочої поверхні .

Розробка композиційних контактних матеріалів на основі срібла з оксидними та тугоплавкими інгредієнтами.

Прототипом для створення дослідних КМ є відомий спечений контактний матеріал Ag-SnO_2.

Контактний матеріал на основі Ag-SnO_2 (срібло-оксид олова) є одним із перспективних матеріалів для заміни контактів з наявним у них оксидом кадмію (CdO). Матеріал Ag-SnO_2 має високу ерозійну стійкість та високий опір зварюванню.

Основний недолік цього матеріалу – утворення на робочій поверхні контакту термостабільного шару з високим питомим опором, що призводить до перегріву контактів при довготривалих навантаженнях, що знижує електроерозійну стійкість, надійність та термін служби апаратів.

Дослідження показали, що термостабільний шар утворюється частинками SnO_2, які виштовхуються на поверхню контакту розплавленим дугою сріблом.

Запобігання утворенню термостабільного шару забезпечує введення невеликої кількості за масою оксиду вольфраму (WO_3). Розплавлені частинки оксиду вольфраму ($T_{пл}$ = 1470 °C) покривають тверді частинки оксиду олова ($T_{пл}$ = 1900 °C) та утворюють волокнистість розплавленого срібла, де волокнами є частинки оксиду олова, покриті розплавленим оксидом вольфраму. Завдяки волокнистій структурі розплавленого срібла електроерозійна стійкість матеріалу підвищується.

Для матеріалів з гетерогенною мікроструктурою встановлена закономірність закріплення основи дуги в районі границь структурних складових, де полегшуються умови виникнення автоемісійних центрів.

Структурною складовою, що виконує дугогасильні функції розробленого композиційного контактного матеріалу, є цирконій (Zr). Цирконій підвищує електроерозійну

стійкість контактного матеріалу за рахунок поглинання кисню із розплавленого срібла під дією електричної дуги, що призводить до зменшення часу горіння дуги та розбризкування рідкого срібла.

Введення оксиду індію (In_2O_3) дозволяє рівномірно розподіляти дрібнозернисті оксиди олова в срібній матриці та прискорювати дифузію олова в срібну матрицю при виготовленні контактного матеріалу, що підвищує твердість розроблюваного матеріалу.

Електрична дуга закріплюється на найменш електро- і теплопровідному інгредієнті – оксиді олова, і при переміщенні з одного його включення на інше по робочій поверхні контакт-деталі відбувається дисипація енергії електричної дуги, і кількість теплової енергії, яка потрапляє до внутрішньої частини композиційного контактного матеріалу, значно знижується, що впливає на підвищення електроерозійної стійкості контакт-деталей.

Електро- і теплопровідна фаза на основі срібла, що знаходиться з боку від стовпа дуги, який закріплений на термостабільному інгредієнті оксиді олова, відводить теплову енергію від зони дії основи дуги, що зменшує розміри ділянки плавлення і випаровування.

Інгредієнти для даного композиційного матеріалу підбиралися з такими властивостями, щоб розв'язувати конкретну задачу: підвищити екологічну безпеку магнітних пускачів і їх електроерозійну стійкість.

Технологія виготовлення нового екологічно безпечного та ерозієстійкого контактного матеріалу.

Використання технології порошкової металургії та внутрішнього окиснення інгредієнтів композиційного контактного матеріалу дозволяє створити контактний матеріал складної будови, що складається з декількох частин, кожна з яких має своє функціональне призначення: підвищувати електроерозійну стійкість, володіти високими дугогасильними властивостями, стабілізувати перехідний контактний опір, протидіяти зварюванню контакт-деталей.

Принциповими моментами технології виробництва електроконтактних матеріалів методами порошкової металургії та внутрішнього окиснення є:

- отримання порошків необхідного хімічного та гранулометричного складу, шляхом відновлення суміші порошків в газовому середовищі;

- внутрішнє окислення домішок порошків, які входять як складові в матеріал на основі срібла;

- формування із цих порошків заготовок відповідного розміру та форми, пресування;

- перетворення заготовок у практично безпористі вироби шляхом спікання в контрольованих газових середовищах;

- температурна обробка та формування кінцевих розмірів та структури.

Вихідними матеріалами для виготовлення дослідного екологічнобезпечного та ерозієстійкого композиційного матеріалу методом внутрішнього окиснення були наступні порошки: срібло Ag, оксид олова SnO_2, оксид індію In_2O_3, які змішувалися в заданій пропорції в стальному циліндричному барабані в сухому вигляді.

По закінченні змішування добавлявся 3 % розчин полівінілового спирту у воду з розрахунку 8..10 мл розчину на 100 гр маси суміші.

Суміш срібла з оксидами піддавалася відновленню в атмосфері водню. Температура відновлення становила 650 °С, час витримки складав 3 години.

Охолоджена суміш протиралась через сито № 01. Отримані порошки сплавів срібло-олово-індій піддавалися внутрішньому окисненню. Для внутрішнього окиснення необхідний дифузійний потік кисню із зовнішнього середовища через срібну матрицю сплаву.

Порошок розподілився тонким шаром 1..1,5 мм у човнику із нержавіючої сталі, яка завантажувалася в трубчасту піч, через яку пропускався кисень.

Температура окиснення складала 700 °С, час витримки – 2 години.

Після окиснення порошок подрібнювався до 30 мікронів. Після чого, до окиснених порошків срібло-оксид олова-оксид індію додавалося 2 % маси цирконію і 0,5 % маси оксиду вольфраму.

Для виготовлення суміші контактного шару матеріалу з наступними складовими: 82 % маси Ag + 11,5 % SnO_2+ 4 % In_2O_3 + 2 % Zr + 0,5 % WO_3, використовувався стальний барабан об’ємом $5 \cdot 10^3$ $см^3$ зі стальними кульками. Час змішування дорівнював 4 години, який забезпечував рівномірний розподіл інгредієнтів.

Контакти спікалися в повітряній атмосфері при температурі 900 °С протягом години, допресовувалися при 6 МПа, повторно спікалися при 800 °С протягом години, калібрувалися при тиску 9 МПа і відпалювалися при 500 °С протягом години.

Тиск пресування суміші для виготовлення дослідних зразків контакт-деталей становив 50..80 МПа.

Унаслідок даної технології виготовлення було отримано очікувану мікроструктуру з рівномірним розподілом у срібній матриці інгредієнтів, що відіграють роль дисперсно-керуючих домішок.

Електрична дуга закріплюється на найменш електро- і теплопровідних включеннях, і кількість теплової енергії, яка потрапляє до композиційного контактного матеріалу знижується, що впливає на підвищення електроерозійної стійкості контакт-деталей.

Висновок.

Проведений огляд контактних матеріалів низьковольтних комутаційних апаратів показує, що створення більш універсальних матеріалів на сьогодні пов'язане з розробкою гетерогенних систем – композиційних матеріалів, компоненти яких, не змішуючись один з одним, забезпечували б необхідний набір властивостей, які висувають до електричних контактів комутаційних апаратів.

У пускачах і контакторах, зокрема у магнітних пускачах типу ПМЕ, ПМА, ПМЛ, застосовуються металокерамічні контакти марки КМК-А10м, які мають у своєму складі токсичний оксид кадмію (CdO), завдяки якому суттєво збільшується електрична зносостійкість контактів. Екологічне законодавство на сьогодні забороняє у виробах електротехнічного призначення застосування кадмію та його сполук.

Дослідження, проведені науковцями у різних країнах, показали можливість застосування в електричних контактах на основі срібла, замість оксиду кадмію, оксидів інших металів, зокрема оксид олова.

Проведений аналіз патентної та наукової літератури визначив основний напрям досліджень, який полягає в обґрунтуванні методів вибору інгредієнтів та технології виготовлення композиційних контактних матеріалів на основі срібла, з метою забезпечення екологічної чистоти і високої електроерозійної стійкості контактної системи магнітних пускачів.

Контактний матеріал на основі Ag-SnO_2 (срібло-оксид олова) є одним із перспективних матеріалів для заміни контактів з наявним у них оксидом кадмію (CdO). Матеріал Ag-SnO_2 має високу ерозійну стійкість та високий опір зварювання. Основний недолік цього матеріалу – утворення на робочій поверхні контактного шару термостабільного оксиду олова з високим питомим опором, що призводить до перегріву контактів при тривалому протіканні через робочі поверхні струму. Цей недолік можна усунути введенням невеликих за масою домішок оксиду вольфраму (WO_3), оксиду індію (In_2O_3) та цирконію (Zr).

Технологія порошкової металургії та внутрішнього окиснення дозволила створити контактний матеріал 82 % Ag – 11,5 % SnO_2 – 4 % In_2O_3 – 2 % Zr – 0,5 % WO_3 з рівномірним розподілом у срібній матриці інгредієнтів, що відіграють роль дисперсно-керуючих домішок, функціональне призначення яких підвищувати електроерозійну стійкість, мати високі дугогасильні властивості, стабілізувати перехідний контактний опір, протидіяти зварюванню контакт-деталей.

Економічна ефективність застосування розроблених композиційних контактних матеріалів досягається за рахунок меншої вартості контакт-деталей, збільшення терміну служби контакт-деталей (приблизно в 1,7 рази) та можливістю зменшити масу контактів

приблизно на 37 %, що дозволить зберегти дорогоцінний матеріал – срібло, та знизити собівартість магнітного пускача.

References:

Державні санітарні правила та норми України. № 2.2.7. 029-99. – Додаток 2, п.22.- с. 8.
2.https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:037:0019:0023:en:PDF
https://www.unep.org/environmentassembly/
Braunovic M. Power connections / M. Braunovic // Electrical contacts: principles and applications. Slade P.G., ed. New York: Marcel Dekker, Inc. 1999. – p. 155 .
Заявка 4042184 ФРН, МК^5 H01 H 1/00. Verfahren und Anordnung zur Strombelastung von elektrischen Kontakten / Hertel Wolfgang, Schedler Dietmar; Schiffselektronik Rostok GmBH. - №4042184.8; Заявл. 29.12.2020; Опубл. 2.7.2022.
Braunovic M. Electrical contacts: fundamentals, applications and technology / M. Braunovic, V.V. Konchits, N.K. Myshkin. – New York: CRC Press, 2019. – p.468.
Buldum A. Contact resistance between nanotubes / A. Buldum, J.-P. Lu // Phys. Rev, 2021. B63. – p.p. 16-26.
Johler W. Switching contacts for low level applications / W. Johler // Proceedings of 21st International Conference on Electrical Contacts. – Zurich, Switzerland, 2002. – p. 147.
Hartmann U. Magnetic multilayers and giant magnetoresistance, fundamentals and industrial applications / Hartmann U. – Springer Verlag, 2010. – p.254.
ДСТУ 2848-94 Апарати електричні комутаційні. Основні поняття. терміни та визначення. – [Дійсний від 01.01.1996].
Контакт-детали металлокерамические: ТУ 16-685.020-85.
Lindmayer M., Bohm W., Geschaftbereich, Technische Metallerzeugnisse und Forschung Metall. D 6450 Hanau (FRG). Effect of Alkali on the switching behavior of Ag-CdO // Proc. of the 10-th Internationfl Conference on Electrical Contact, Phenomena. – 2010. – p.860.
ТУ 16-685.026-96. Композиційний матеріал типу СрН-10: на заміну ТУ 16-685.020-85. – [від 01.01.1996].
Пат. 4846901 США, МКИ4 С 23 С 8/10. Method of making improved silver-tin-indium contact material / Lima Antonio E., Shen Yuan; Engelhard Corp.-№129272; Заявл. 07.12.2017; Опубл. 11.07.2019; НК 148/13.1. – p. 8.
Muller K, Stockei D, Rau G. The IRE Process for the Manufacture of Silverbased Composite Contact Materials // Proceedings of International Conference on Electric Contact and Annual Holm Conference on Electrical Contacts, sept. 17-21, 2015. – Chicago , Illinois. – p. 237-242.
Контактори електромагнітні низьковольтні. Загальні технічні умови : ДСТУ 2846-94 . – [чинний від 01.01.1996]. – К.: Держспоживстандарт України, 1996. – 18 с. – (Національні стандарти України).
Апарати електричні низьковольтні. Методи випробувань : ДСТУ 2993-95. – [чинний від 01.01.1996]. – К.: Держспоживстандарт України, 1996. – 112 с. – (Національні стандарти України).
Апарати комутаційні низьковольтні. Загальні технічні умови: ДСТУ 3020-95. – На заміну ГОСТ 12434-93. – [чинний від 01.01.1997].– К.: Держспоживстандарт України, 2006. – 18 с. – (Національні стандарти України).
Матеріали металеві спечені, крім твердих сплавів. Зразки для випробування на розтяг: ДСТУ 3670-97 (ISO 2740-86). – [чинний від 01.07.1999]. – К.: Держспоживстандарт України, 2000. – 15 с. – (Національні стандарти України).
Зносостійкість виробів. Тертя, зношування та змащування. Терміни та визначення: ДСТУ 2823-94. – [чинний від 01.01.1996]. – К.: Держспоживстандарт України, 1996. – 12 с. – (Національні стандарти України).

DOI 10.5281/zenodo.10821982

UDC 656.2:004

CHAPTER 16.
AUTOMATED CONTROL SYSTEMS IN RAILWAY TRANSPORTATION

Hanna KYRYCHENKO

Doctor of Technical Sciences, Professor

State University of Infrastructure and Technologies, Department of Transport Technologies and Transportation Processes Operation,

(9, Kyrylivska Street, Kyiv, 04071, Ukraine)

kyrychenko_gi@gsuite.duit.edu.ua

https://orcid.org/0000-0002-6883-1877

Yuliia BERDNYCHENKO

Candidate of Historical Sciences, Associate Professor

State University of Infrastructure and Technologies, Department of Transport Technologies and Transportation Processes Operation,

(9, Kyrylivska Street, Kyiv, 04071, Ukraine)

berdnichenko_ya@gsuite.duit.edu.ua

https://orcid.org/0000-0001-7536-7155

Abstract. Management of freight transportation in Ukrainian railways no longer exists without the use of automated systems. It can be observed that all technologies developed and implemented in management processes are realized only in the informational environment. In particular, accounting for the work of departments and the entire railway, calculation of quantitative and qualitative indicators of departmental and overall railway performance, financial and accounting reporting, technological documents, billing documents for services provided, and other activities take place in the information base - the unified automated management system for freight transportation of Ukrzaliznytsia (ASC FT UZ-E). The paper presents the results of analysis and theoretical generalization of scientific works addressing the problems of the functioning automated railway system. A multitude of models of the transportation process (informational images of management objects) is considered, forming the logical database that ensures the unity of the information environment of the automated freight transportation management system of Ukrzaliznytsia (ASC FT UZ-E).

Keywords: information technologies; railway; station; transportation; models.

АВТОМАТИЗОВАНІ СИСТЕМИ УПРАВЛІННЯ НА ЗАЛІЗНИЧНОМУ ТРАНСПОРТІ

Анотація. Управління вантажними перевезеннями залізниць України вже не існує без використання автоматизованих систем. Можна констатувати, що всі технології, які розроблюються та впроваджуються у процеси управління реалізовуються тільки у інформаційному середовище. Зокрема облік роботи підрозділів і всієї залізниці, розрахунок кількісних та якісних показників роботи підрозділів та всієї залізниці у цілому, фінансова та облікова звітність, технологічні документи, розрахункові документи за наданні послуги та інше відбувається у інформаційній базі – єдиній автоматизованій системи управління вантажними перевезеннями Укрзалізниці (АСК ВП УЗ-Є). У роботі наведено результати аналізу і теоретичного узагальнення наукових праць, у яких розглядаються проблеми функціонуючої автоматизованої системи залізниці. Розглянуто множину моделей перевізного процесу (інформаційних образів об'єктів управління), яка складає логічну базу даних, що забезпечує єдність інформаційного середовища автоматизованої системи керування вантажними перевезеннями Укрзалізниці (АСК ВП УЗ-Є).

Ключові слова: інформаційні технології; залізниця; станція; перевезення; моделі.

Вступ. Транспортний сектор України відіграє важливу роль у соціально – економічному розвитку країни, адже розвинута транспортна система є передумовою економічного зростання, підвищення конкурентоспроможності національної економіки і якості життя населення. Україна володіє розвинутою інфраструктурою залізничного транспорту, за довжиною мережі залізниць Україна посідає друге місце у Європі – 21,7 тис. км. Для сприяння розвитку країни залізничний транспорт повинен розвиватися випереджальними темпами. З цією метою державою була розроблена Транспортна стратегія, де позначені проблеми транспорту та намічені цілі, пріоритети та визначені основні напрямки реалізації стратегії.

Серед проблем зазначено відставання в розвитку транспортно – логістичних технологій, мультимодальних перевезень, рівня контейнеризації, все це зумовлює високу частку транспортних витрат у собівартості перевезень, а це означає зниження конкурентоспроможності національно транспорту і залізничного зокрема.

Тому серед основних цілей розвитку визначено забезпечення конкурентоспроможності та якості транспортних послуг для економіки та доступності та якості для населення.

Серед напрямків, за якими передбачено вдосконалювати роботу транспорту визначені наступні:

- збільшення пропускної спроможності транспортної інфраструктури;

- створення логістичних центрів;
- удосконалення інформаційно – комунікаційних технологій;
- створення комплексних інформаційних систем управління, інтелектуальних транспортних систем.

Втілення цих заходів висуває нові вимоги до системи управління залізничним перевезеннями, до її взаємодії з системами управління промисловими підприємствами та інших видів транспорту. Такі системи координації потребують ефективного управління багатьма об'єктами. Їх реалізація не можлива без інформації про стан об'єктів, прогнозу процесів з об'єктами, а значить і без автоматизації систем управління.

Автоматизовані системи і інформаційні технології: основні поняття і напрямки розвитку. На залізницях України функціонують сотні тисяч об'єктів управління близько однієї тисячі станцій, десятки локомотивних, вагонних депо, дирекції перевезень, дільниці на дирекціях, залізниці, кілька тисяч локомотивів, сотні тисяч вагонів (з кількома десятками їх власників) і все це потребує управління на мережі довжиною 21,7 тис. кілометрів. Тому сучасний рівень управління потребує створення апарату точних наук та методів їх використання на практиці, це пов'язано з розвитком кібернетики, методів дослідження операцій, які базуються на кількісних характеристиках процесів. Такі характеристики отримуються з інформаційних автоматизованих систем.

На залізничному транспорті функціонують автоматизовані системи різних рівнів управління: системи управління вантажними перевезеннями, продажем місць у пасажирських перевезеннях, управління сортувальною роботою станції, системи управління гірковими пристроями, системи матеріально – технічного забезпечення, системи обробки даних про роботу локомотивів та машиністів, локальні автоматизовані системи окремих процесів – нормування, обліку, фінансового, кадрового забезпечення, складання графіку руху поїздів, плану формування поїздів, проведення окремих інженерних розрахунків, система електронного документообігу працівників залізниці, а також системи зчитування інформації

У всіх перелічених системах оброблюється інформація про об'єкти управління залізничного транспорту. До об'єктів автоматизованих систем відносяться об'єкти управління на залізниці: вантажна відправка; контейнер; вагон, локомотив; поїзд; колія; станційний парк; станція; вагонне депо; локомотивне депо; контейнерний майданчик; під'їзна колія; диспетчерська дільниця; дирекція, залізниця, залізнична адміністрація; користувач залізничних послуг (*Науменко П., Миненко В., Землянов В., 2007*).

Для безпосередньої та оперативної участі в управлінні вантажними перевезеннями близько 30 років тому в Проектно – конструкторському технологічному бюро була створена

Автоматизована система оперативного управління перевезеннями – АСОУП. Розвиток цієї системи на залізницях України привів до створення та впровадження в управлінні вантажними перевезеннями системи АСК ВП УЗ, а пізніше АСК ВП УЗ-Є (*Башлаєв В., Цейтлін С., Великодний В., 2007*).

Принципова відміна системи АСКВП УЗ від АСОУП в наявності інформації про вантаж, а саме: номер відправки, характеристики вантажу, коди, назва, інформація про пломби, охорону вантажу, цінність та інші. Саме тому впровадження та розширення функцій АСК ВП УЗ дає можливість управляти перевезеннями на підставі даних про вантаж (саме це важливе для клієнта залізниці), тобто забезпечити конкурентоспроможність та якість транспортних послуг для економіки, доступності і якості для населення.

Зараз АСК ВП УЗ-Є на мережі залізниць обслуговує більш ніж 12,5 тис. користувачів, щодобово обробляє 457 тис. технологічних документів, створює більш 500 тис. довідок та звітів, що забезпечують управління галуззю (*Цейтлін С., Коваленко Л., Николєнко М., 2015*).

Автоматизована система залізниці містить інформацію про події з об'єктами управління, такими як вантаж, вагон, поїзд, колія, залізниця, станція, вантажні райони, диспетчерська дільниця, дирекція, УЗ (*Цейтлін С., Подоляк С., Василишин І., 2015*).

Автоматизовані системи, що функціонують на залізниці поділяються за призначенням, видом використання, набором функцій по класах (рис.1).

АСК ВП УЗ – автоматизована система управління вантажними перевезеннями. Дає можливість вести поїзну, контейнерну, локомотивну моделі залізниці з передачею інформації в аналогічні моделі рівня Укрзалізниці. Це дозволяє вести оперативний контроль навантаження і вивантаження вагонів і контейнерів, дислокацію локомотивів і локомотивних бригад, контроль прослідування пасажирських поїздів, облік і видачу попереджень в поїзній роботі.

АСК ПП УЗ – автоматизована система управління пасажирськими перевезеннями, яка виконує функції бронювання і централізованого продажу проїзних документів, управління багажними операціями сервісного обслуговування.

АСБО «ФОБОС» – автоматизована система бухгалтерского обліку призначена для автоматизації бухгалтерского обліку на підприємствах залізниці.

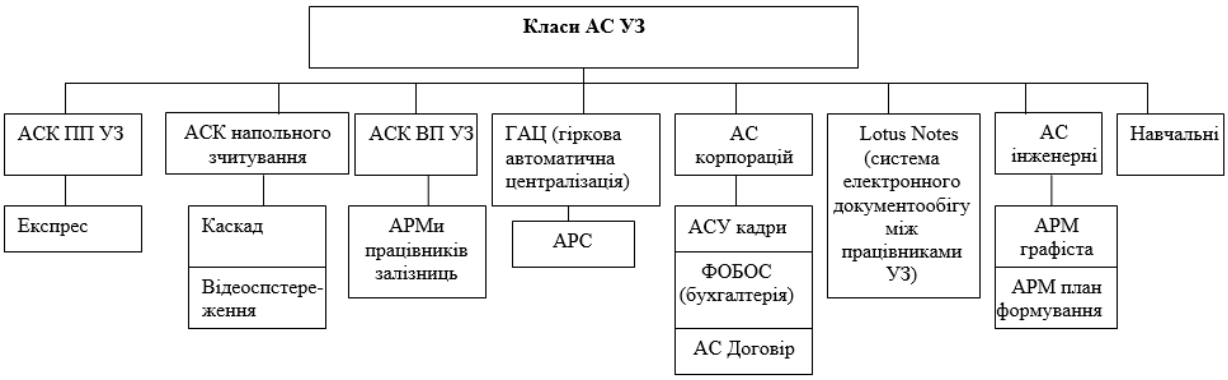


Рисунок 1 – Класи автоматизованих систем

Моделі перевізного процесу. Інформація про події з об’єктами управління передається з АРМів працівників залізниць до центральної бази даних про перевізний процес АСК ВП УЗ-Є, де оброблюється, зберігається та утворює окремі моделі перевізного процесу.

Ці моделі є віртуальними (не існуючі фізично) і мають зміст:

1. Поїзна модель (інформація про вагони, локомотиви, локомотивні бригади).
2. Локомотивна модель (локомотиви, поїзди, час роботи локомотивних бригад, ремонт локомотивів).
3. Вагонна модель (всі події з вагонами).
4. Модель п/к (умови договорів залізниці та підприємств; вагони, що знаходяться на підприємстві).
5. Модель нарахувань (всі нарахування за перевезення).
6. Контейнерна модель (вагони, контейнери, вантажі).
7. Відправочна модель (всі відправки, перевізні документи).

Моделі знаходяться у взаємодії, у строгій ієрархії по законах логічних контролів та за вимогами діючих законів, нормативів, наказів, інструкцій тощо. (рис. 2).

Множина моделей перевізного процесу (інформаційних образів об’єктів управління) складає логічну базу даних (ЛБД), що забезпечує єдність інформаційного середовища АСК ВП УЗ-Є. Моделі зв’язані між собою різними відношеннями, але будуються за єдиною формальною схемою, що спирається на чотири базових типа:

- простий об’єкт – не змінюється впродовж всього періоду свого існування (життєвого циклу);
- змінний об’єкт (розвиток простого) – може змінювати свій стан впродовж життєвого циклу;

- рухомий об’єкт (розвиток змінного) – може переміщуватися між полігонами різних стаціонарних об’єктів (змінює дислокацію);

- стаціонарний об’єкт (розвиток змінного) – має полігон, топологічні зв’язки (примикання) з полігонами інших стаціонарних об’єктів.

Кожна модель (її стан) характеризується множиною атрибутів, які поділяються на групи, що не пересікаються між собою – грані моделі, вони можуть містити внутрішні грані (під грані). Склад граней та атрибутів для кожної моделі специфічний, але можуть існувати типові грані та атрибути, які характерні для базового типу у цілому. Таки чином, всі моделі обов’язково включають так звану головну грань, що містить унікальний ідентифікатор об’єкта та його життєвий цикл, всі змінні моделі включають грань операцій з об’єктами даного типу, всі рухомі об’єкти мають дислокаційну грань і т. п. (*Кириченко Г., 2017*).

Зв’язки між моделями організуються чи як посилання із грані однієї моделі на ідентифікатор об’єкта іншої, чи введенням підграні, загальної для двох граней різних моделей (*Кириченко Г., 2021*). Зведення всіх даних АСК ВП УЗ-Є до типових моделей та зв’язкам між ними забезпечує:

- інтеграцію всіх даних системи, що дає можливість обирати будь-яку комбінацію даних різних об’єктів, пов’язаних різними зв’язками;
- принципову відкритість бази даних БД для розширення – додавання до БД нової моделі практично не впливає на функціонування вже існуючих;
- типізацію та універсалізацію процесів запису та читання даних з моделей, а також полегшує їх супровід (розвиток, виправлення помилок і т.п.).

База даних кожного вузла в загальному випадку відображає свій фрагмент ЛБД-підмножину моделей, їх граней та атрибутів цих граней.

Вагонна модель, її опис. Вагонна модель містить у собі інформацію про вагони: картотечні дані про вагон, інформацію про рейси вагона по залізниці, про зміну картотечних даних під час перебування вагона на залізниці, технічний стан, стан з завантаження, призначення, дислокація, всі операції з вагоном на полігоні залізниці.

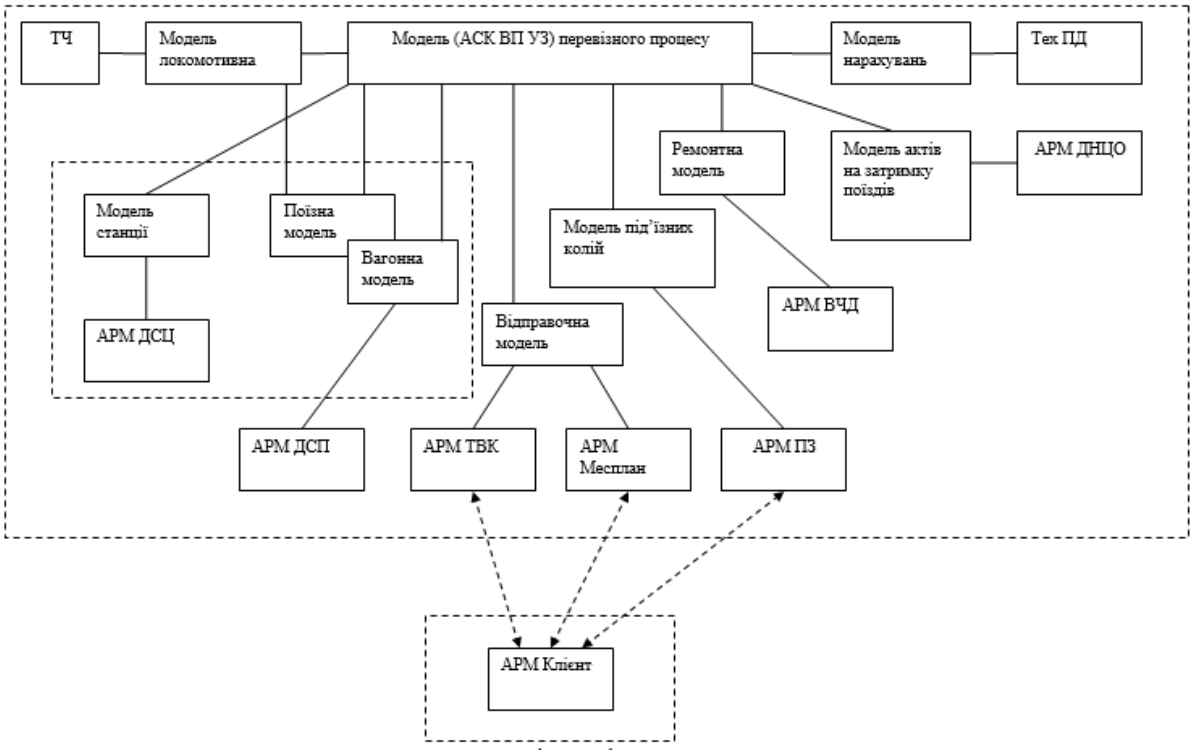


Рисунок 2 – Структурна схема АСКВПУЗ-Є

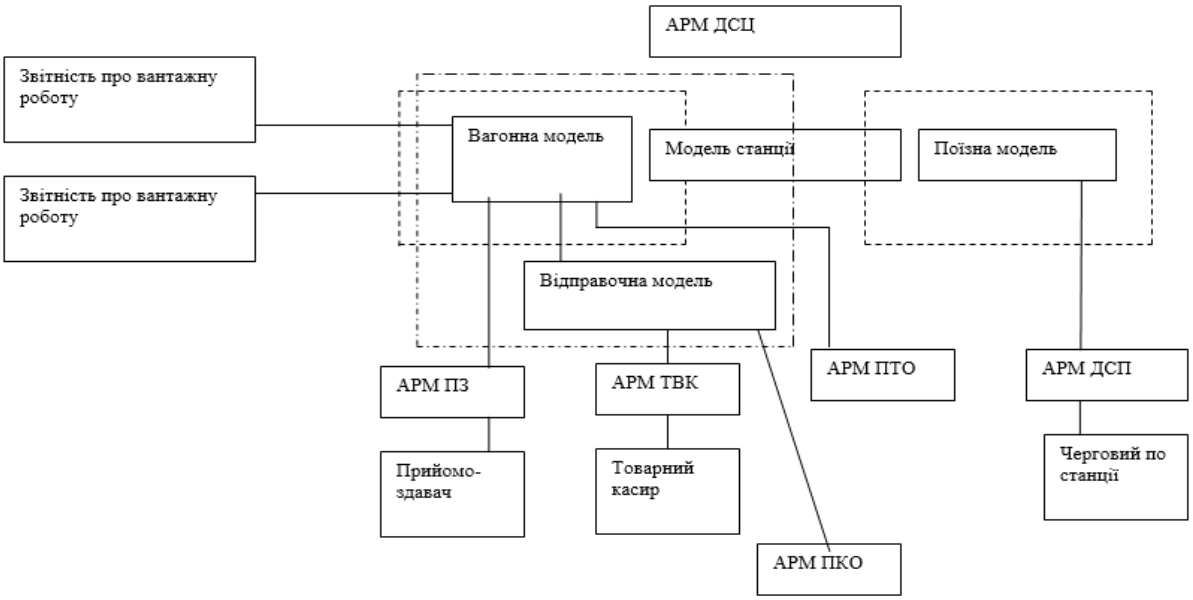


Рисунок 3 – Інформаційна модель станції

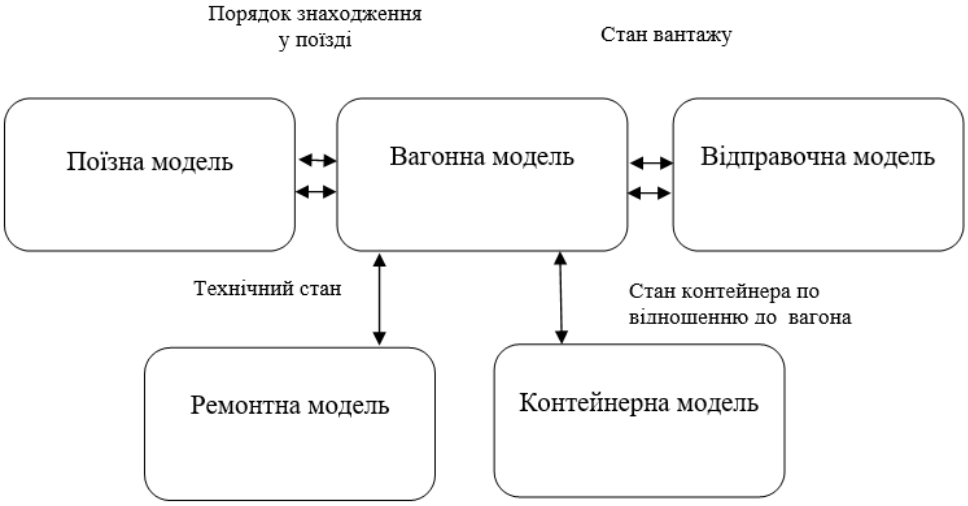


Рисунок 4 – Взаємодія вагонної моделі з іншими моделями перевізного процесу

Зв'язок з іншими моделями. Вагонна модель зв’язана з наступними моделями (рис.4):

- поїзна модель – зв’язок здійснюється через ідентифікатор стану дислокаційної грані вагону за допомогою таблиці зв’язку LINK_POIZD_VAG (нумерація вагонів у поїзді);
- відправочна модель – зв’язок здійснюється через ідентифікатор стану грані навантаження вагона за допомогою таблиці зв’язку LINK_VAG_OTPR (код документа 050104.0.13.01.0.002);
- контейнерна модель – зв’язок здійснюється через ідентифікатор стану грані навантаження вагона за допомогою таблиці зв’язку LINK_VAG_CONT (код документа 050103.0.13.01.0.001);
- ремонтна модель вагонного депо – зв’язок здійснюється через ідентифікатор стану грані технічного стану вагона за допомогою таблиці зв’язку LINK_VAG_VCHD (код документа 050113.0.13.01.0.001).

Головна таблиця вагонної моделі. Містить тільки стандартні атрибути – абсолютний ідентифікатор та життєвий цикл об’єкту, ідентифікатор об’єкта, час початку життєвого циклу об’єкта, час кінця життєвого циклу об’єкта.

Таблиця, що містить дані про операції з вагонами: ідентифікатор операції, час здійснення операції.

Таблиця, яка відображає стан технологічного ідентифікатору вагону інвентарного номер: час початку запису, час кінця запису.

Таблиця, яка відображає дислокацію вагону:

201 – станція;

203 – під’їзна колія;

204 – вагонне депо;

110 – поїзд

Таблиця, яка відображає дані про курсування вагону на залізниці: пробіг вагона в навантаженому стані, пробіг вагона в порожньому стані.

Таблиця, яка відображає інформацію про порушення плану формування: нормативний стик здачі вагона, стик здачі вагона.

Вагона модель будується на інформації про події з вагоном у поїздах та операціях з вагоном на станціях.

З відповідних моделей дані про операції записуються до вагонної моделі, події у всіх моделях зв'язані послідовністю операцій у вагонній моделі.

Оперативне введення інформації про поїзди відбувається з поїзної моделі, де здійснюється проведення всіх логічних контролів введених даних, контролю послідовності операцій з поїздом та вагонами по БД і моделях системи, формується діагностика про результати контролю, розрахунок і занесення інформації до всіх необхідних моделей системи АСК ВП УЗ-Є.

Поїзна модель наповняє базу інформацією: про склад поїзда, коригування складу поїзда, відправлення поїзда, прибуття поїзда, про прослідування поїздом станції без зупинки, про підготовку поїзда до відправлення, про розформування вантажного поїзда, про тимчасову зупинку («кидання»), про об'єднання і роз'єднання составів вантажного поїзда, про зміну індексу вантажного поїзда, про операцію з поїздом при обміні інформацією між сусідніми залізницями.

Операції з вагоном на станції:

- відчеплення - причеплення,
- перестановка,
- подавання-забирання,
- подавання – забирання у ремонт /з ремонту

Динамічна модель станції. Комплекс 4007 – «Керування станцією».

Система включає наступні задачі:

- 400701 – «Обробка інформації про склад поїзду по прибуттю»;
- 400702 – «Розрахунок і формування документів для розформування поїзда»;
- 400703 – «Розрахунок і видача документів на сформовані поїзди»;
- 400704 – «Оперативне коректування спеціалізації колій сортувального парку»;
- 400705 – «Контроль за дислокацією вагонів на коліях і в парках станції»;
- 400706 – «Формування оперативної звітності про роботу станції»;

- видача інформації про поїзди і вагони, що знаходяться на коліях парків прийому і відправлення і про вагони, що знаходяться на коліях сортувального парку;
- формування і розрахунок довідки про роботу сортувальних гірок на підставі даних про загальну кількість розформованих поїздів;
- формування і розрахунок довідки про наявність на станції транзитних вагонів із переробкою і порожніх вагонів по родам.
- 400707 – «Формування і видача попереджень на поїзд, що відправляється»;
- 400708 – «Ведення настільного і балансового журналів роботи станції».

Опис моделі станції. Модель станції в автоматизованій системі реалізується за допомогою таблиць, данні яких відображають характеристики підсистем та пов'язані між собою. Модель вводиться для реалізації поїзної та вагонної моделі АСК ВП УЗ-Є у частині визначення місцезнаходження поїздів та вагонів на коліях станції. Таким чином можна сказати, що модель станції складається з двох частин: комплекс таблиць з описом стаціонарних характеристик та комплекс даних про об'єкти управління, що динамічно змінюються (*Кириченко Г., Стрелко О., Бердниченко Ю., Макарова О., 2013*).

Таблиця опису топології та характеру роботи станції призначена для опису незмінних характеристик станції. Таблиця містить у собі відомості про станцію: початкову інформацію – код, назву, скорочену умовну назву; інформацію про напрямки відправлення і прибуття; інформацію про призначення плану формування, інформацію про комерційні операції і про ознаки роботи.

Таблиця опису топології та характеру роботи станції, №1 – ідентифікатор станції містить:

- назва станції;
- напрямки;
- напрямок 1;
- назва напрямку;
- напрямок 2;
- назва напрямку;

Перелік операцій з вагоном та вантажем на станції: вантажні роботи, вивіз контейнерів, робота на під'їзних коліях і т.д.

Дані плану формування:

призначення 4800 – 5399 на 4402 – Основа Осн

3700 – 3705 - 3704 – Кліпарів Кліпр

3200 – 3200 - 3200 – Місцеві місц

Динамічна модель станції – це вагонна модель станційних колій для формування технологічних документів станції (*Kyrychenko H., Strelko O., Berdnychenko Yu., Hurinchuk S., 2018*). Вона складається з таблиць, у складі яких зазначаються змінні реквізити – характеристики експлуатаційної роботи станції.

Таблиця моделі станційних колій, №2: ідентифікатор об'єкту:

- дата початку життєвого циклу об'єкту;
- дата кінця життєвого циклу об'єкту;
- номер колії;
- номер парку на станції, до якого належить колія;
- місткість колії у вагонах.

Наявність бази даних та прикладне програмне забезпечення реалізують наступні функції АС:

- складання та видача розміченого натурного листа;
- складання та видача сортувального листа;
- облік накопичення вагонів на коліях сортувальних та прийомо - відправочних парків;
- автоматичне формування натурного листа поїзда по відправленні;
- поточне планування поїздоутворення за періодами доби;
- аналіз вагонопотоків і виявлення порушень потоків планоформування;
- можливість формування поїзда за вимогами терміну доставки;
- можливість формування поїзда за визначеними диспетчерським апаратом умовами,
- облік наявності поїздів та вагонів в парках станцій і роботи з ними;
- складання форм станційної звітності ДО-2 і ДО-6; ДУ -2, 3, 4
- інформаційне обслуговування працівників станції.

Інформаційні потоки між АРМами працівників, що утворюють моделі перевізного процесу наведені на рис. 5.

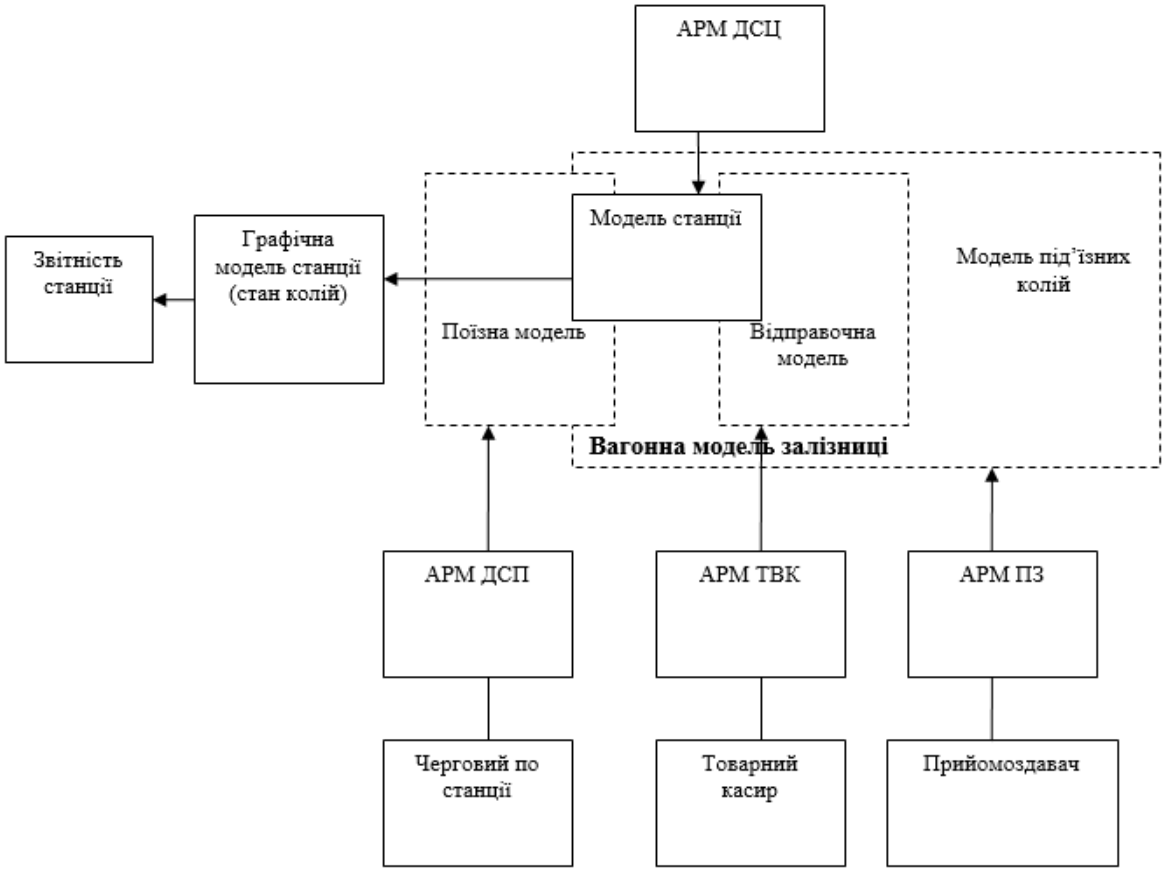


Рисунок 5 – Схема інформаційних потоків на станції

Технологічна схема інформаційної обробки поїздів. Повідомлення про події з поїздом в автоматизованих системах повинні відповідати фактичним подіям, які здійснюються у житті:

t1 – прибуття поїзда;

t2 – списування по прибуттю номерів вагонів;

t3 – корегування складу поїзда у ТГНЛ для точного розрахунку розміченої ТГНЛ та сортувального листа;

t4 – комерційний огляд;

t5 – ТО та передача його результатів до ремонтної або вагонної моделі;

t6, t7, – час закінчення операцій комерційного та технічного огляду з відповідним наданням результатів до моделі АСК ВП УЗ-Є;

t8 – маневрові операції з поїздом та корегування складу поїзда, інформація про вантаж;

t9 – розрахунок технологічних документів для подальшої обробки поїзда;

t10 – розформування поїзду відповідно із складеним планом;

t11 – маневрові операції, переставлення вагонів по коліях сортувального парку, корегування вагонної моделі сортувальних колій за рахунок розпуску вагонів;

t12 – час закінчення накопичення складу поїзду на сортувальних коліях або на сортувально-відправочних коліях. Відбувається розрахунок натурного листа нового сформованого поїзду;

t13 – час забирання несправних вагонів на об'єкти ВЧД;

t14 – час подавання вагонів на п/к;

t15 – час повернення вагонів після ремонту;

t16 – час забирання вагонів з п/к;

t17 – розрахунок довідки машиністу для випробування гальм;

t18 – відправлення поїзда;

t19 – час операцій списування поїзда по відправленню та корегування складу поїзда;

t20 – передача інформації про зміну складу поїзду до АСК ВП УЗ-Є для корегування поїзда по відправленню.

Таблиця 1 – Повідомлення в автоматизованих системах

Код повідомлення	Код операції	Опис повідомлення
02		Телеграма-натурний лист поїзду
09		Корегування відомостей про склад поїзду
241		Повідомлення про навантаження вагонів
242		Повідомлення про вивантаження вагонів
1397	98	Зарахування вагонів на відповідальність власника
	97	Зняття вагонів з відповідальності власника
	90	Подавання вагонів на під'їзні колії
	91	Забирання вагонів на станцію
200		Відправлення поїзда зі станції
201		Прибуття поїзда на станцію
202		Проходження поїздом станції
203		Розформування поїзду
205		Готовність поїзда до відправлення
209		Зміна індексу поїзда
1341		Про пошкодження вагонів при навантаженні, вивантаженні та маневровій роботі
333		Для відміни помилково переданих і записаних повідомлень

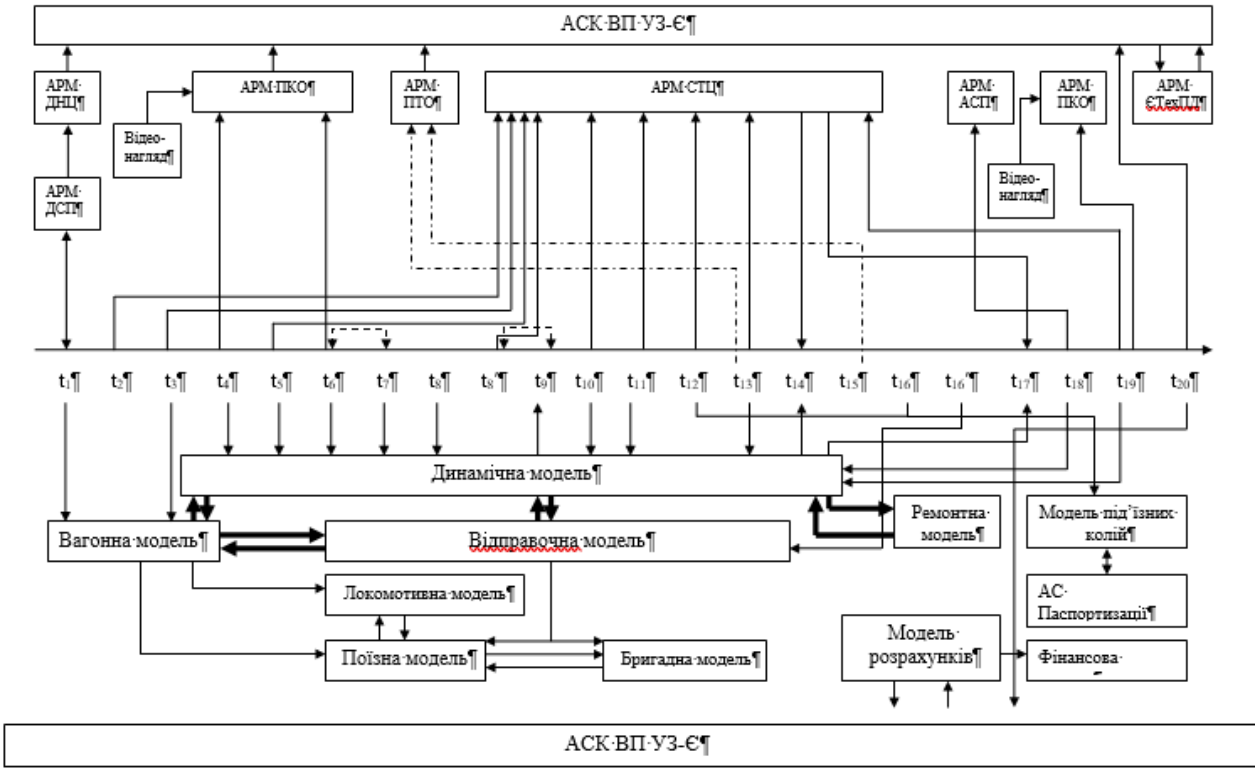


Рисунок 6 – Схема інформаційної обробки поїздів (*Кириченко Г., Бердниченко Ю., 2021*)

Автоматизовані робочі місця працівників комерційного господарства. Комерційний огляд поїздів здійснюється працівниками станцій (приймальниками поїздів, прийомоздавальниками вантажу) на пунктах комерційного огляду – ПКО, які розташовані на залізницях таким чином, щоб була можливість забезпечити комерційний огляд всіх поїздів, що надходять на залізницю і відправляються з неї, а також поїздів що прибувають і відправляються із сортувальних станцій.

Рисунок 7 – Види ПКО

Робота ПКО організовується за технологічним процесом, який є складовою частиною технологічного процесу роботи станції і затверджується наказом начальника Дирекції залізничних перевезень.

Виробничо-технічні приміщення ПКО мають бути обладнані необхідними засобами зв'язку, технічними засобами контролю, забезпечені матеріалами, інструментами і пристосуванням для виявлення та усунення комерційних несправностей.

Для огляду кріплення вантажів на відкритому рухомому складі, перевірки справності покрівлі вагонів і контейнерів, стану люків вагонів і цистерн, наявності залишків вантажів і сміття, не знятих реквізитів кріплення на ПКО мають бути оглядові вишки, обладнані телефонним і радіозв'язком, установками промислового телебачення, іншими технічними засобами.

Для перевірки габариту вантажів на відкритому рухомому складі застосовуються електронні габаритні ворота з дистанційним контролем.

Для пломбування вагонів та контейнерів ПКО забезпечується необхідною кількістю запірно-пломбувальних пристроїв (пломб) та пристосувань для їх навішування і знімання. Розробляються технології з передачі з метою подальшої ідентифікації стану пломб для забезпечення збереженості вантажу.

Загальні вимоги до комерційного огляду поїздів. Поїзди, що прибувають чи відправляються зі станції, оглядаються працівниками ПКО з метою виявлення та усунення комерційних несправностей, що загрожують безпеці руху і збереженню вантажів.

У всіх випадках виявлення комерційних несправностей складається акт загальної форми ГУ-23, який підписується працівниками, що здійснювали комерційний огляд, але не менше двох осіб. Акт загальної форми складається згідно з правилами складання актів.

У разі виявлення вагонів (контейнерів) з ознаками розкрадання вантажу оформляється також третій примірник акта загальної форми, який надається лінійному підрозділу міліції за місцем виявлення ознак розкрадання вантажу.

Про необхідність відчеплення вагонів від поїздів і подачі їх на спеціальні колії для усунення комерційних несправностей або перевірки стану і кількості вантажу працівник ПКО негайно повідомляє чергового по станції (маневрового диспетчера) встановленим порядком, а на вагони наноситься відповідна розмітка.

Порядок усунення комерційних несправностей з відчепленням вагонів від поїзда або без відчеплення, порядок відчеплення вагонів та подачі їх на спеціалізовані колії для усунення комерційних несправностей, порядок обліку таких вагонів і перевірки правильності усунення несправностей встановлюється технологічним процесом роботи станції. Результати огляду кожного поїзда записуються у Книгу реєстрації комерційних несправностей форми ГУ-98. Запис завіряється підписами працівників, що здійснювали огляд. На станціях з інтенсивним рухом поїздів при паперовому оформленні результатів огляду, вони можуть оформлятися після огляду трьох поїздів. ПКО підключаються до мережі АСК ВП УЗ-Є, що дозволяє отримання необхідної інформації з перевізних документів (*Кириченко Г., Габа В., Висоцька Г., 2011*). З цією метою, а також для передачі інформації про комерційний стан вантажів та вагонів після їх огляду розроблена система – АРМ ПКО, автоматизоване робоче місце працівника пункту комерційного огляду.

Автоматизована система забезпечення комерційного огляду вантажів (АРМ ПКО) призначена для автоматизації процесів комерційного огляду поїздів на пунктах комерційного огляду (ПКО).

Основними задачами АРМ ПКО є:

- автоматизований контроль за збереженістю вантажів під час перевезення, забезпечення комерційного огляду вагонів та вантажів з використанням комплексу сучасних технологій – відео спостереження, зважування;

- автоматична передача інформації за результатами огляду про стан вагонів до загальної інформаційної системи станції, що забезпечує неможливість здійснення операцій з вагонами та вантажами, які потребують усунення несправності, особливо з відчепленням;
- надання аналітичної інформації по виявленим комерційним несправностям для прийняття рішення працівником ПКО;
- автоматизоване оформлення обліково-звітної документації;
- автоматична передача інформації щодо комерційних несправностей на рівень залізниці;
- відеоконтроль стану вантажу та його упаковки, цілісності корпусу вагона;
- відеоконтроль наявності запірно-пломбувальних пристроїв на запірних механізмах дверей, люках вагонів, цистерн;
- визначення маси вантажу, зміщення центру маси навантаження під час руху;
- видача повідомлення у разі наявності відхилень від габариту навантаження;
- надання рекомендацій щодо порядку дій при виникненні аварійної ситуації з небезпечним вантажем;
- взаємодія з АСК ВП УЗ-Є у частині обміну інформацією та її обробкою для формування баз даних.

Впровадження АРМ ПКО забезпечує:

- підвищення ефективності та якості роботи працівників ПКО за рахунок використання технічних засобів для виконання операцій комерційних оглядів та обробки інформації за їх результатами;
- підвищення якості експлуатаційної роботи з обробки вагонів та вантажів у комерційному відношенні;
- скорочення часу комерційного огляду поїздів;
- поліпшення умов праці працівників пунктів комерційного огляду;
- підвищення достовірності, повноти та оперативності статистично-звітної інформації, якості її обробки за рахунок реалізації:

а) контролю стану вантажу на відкритому рухомому складі при отриманні працівниками ПКО зображення рухомого складу з телевізійних або цифрових камер безпосередньо на робочому місці;

б) автоматичне списування номерів вагонів;

в) створення баз даних про перевезення вантажу разом із відеозображенням;

г) перегляд відео архівів та пошук інформації за визначеними параметрами;

д) передачу інформації в комерційні служби та в Укрзалізницю;

е) оформлення звітів про виявлені комерційні несправності з роздрукуванням відповідних зображень;

ж) отримання повідомлення про вихід вантажу за межі габариту навантаження;

к) отримання інформації про відповідність фактичної маси вантажу масі, зазначеній в перевізних документах;

л) отримання повідомлення про відхилення центру маси вантажу від повздовжньої та поперечної осі вагона;

м) отримання інформації про порядок дії у разі виникнення аварійної ситуації з небезпечним вантажем;

н) оформлення обліково-звітної документації: акту загальної форми ГУ-23, книги реєстрації комерційних несправностей форми ГУ-98, звіту форми КНО-5 та оперативних телеграм (додатки 1-4), а також, заповнення бланків комерційного акта ГУ-22 або ІНУ-67 (в залежності від виду сполучення).

Технологічні вимоги до системи.

Розробка АРМ ПКО виконане з урахуванням наступних вимог:

- модульної побудови системи;
- високої надійності функціонування інформаційного середовища, достовірності і захищеності інформації;
- підтримки режиму колективного користування ресурсами системи та даними відповідно до встановлених пріоритетів доступу до інформації;
- можливості інтеграції з комплексами зважування та відео спостереження;

Система має складатися з таких структурних одиниць: робоче місце працівника ПКО та серверна частина в рамках сервера застосувань вузла АСК ВП УЗ-Є, забезпечувати можливість взаємодії з іншими інформаційними системами АСК ВП УЗ-Є: АРМ товарного касира, АС під'їзних колій, АС управління актово-претензійною роботою. Забезпечувати взаємодію з програмним забезпеченням автоматичного співставлення маси вантажу визначеної на вагах з масою вантажу вказаного в перевізних документах і, при необхідності, з автоматичною системою контролю габаритів рухомого складу.

Задача повинна бути реалізована як дворівневий комплекс з розмежуванням лінійного рівня та рівня залізниці.

На лінійному рівні впроваджується:

- формування отриманої за допомогою відеокамер інформації в цифровий вигляд та обробка цієї інформації для прийняття рішення працівником ПКО (відчеплення вагона, усунення комерційних несправностей без відчеплення);

- створення архіву відеозображень;
- пошук інформації в базі даних з відправної моделі за визначеними параметрами (№ поїзда, його індекс, № вагона, дата та час, тощо)
- реєстрація комерційних несправностей;

На рівні залізниці провадиться:

- прийом інформації з пунктів комерційного огляду (у вигляді протоколу проходження поїзду);
- пошук інформації за визначеними параметрами (№ поїзда, його індекс, № вагона, дата та час, тощо), можливість друку та передача в електронному вигляді результатів пошуку;
- передача достовірної інформації на рівень Укрзалізниці;
-надійність функціонування задачі, її експлуатаційні характеристики, захист інформації та її збереження повинні відповідати загальним вимогам АСК ВП УЗ-Є.

В рамках системи «Автоматизована система забезпечення комерційного огляду вантажів» реалізовані наступні функції:

- формування протоколу комерційного огляду;
- видача аварійної картки при виникненні аварійної ситуації з небезпечним вантажем;
- ведення книги реєстрації комерційних несправностей;
- формування та облік актів загальної форми;
- складання заготовки для комерційного акту;
- формування і передача оперативних повідомлень (тексту телеграм) щодо незбережених вантажів та комерційних несправностей;
- складання та друк звітів про вагони з комерційними несправностями, виявленими на станції.

При наявності на ПКО однієї, або декількох із зазначених автоматизованих систем: системи відеоконтролю стану вагонів і вантажу, системи визначення ваги вагонів та контролю зміщення центру мас навантаження із застосуванням електронних ваг, системи визначення габаритів вантажу із застосуванням автоматизованих габаритних воріт, дані з цих систем використовуються АС ПКО при формуванні протоколу комерційного огляду.

АС ПКО забезпечує видачу попередження, у вигляді спеціальної позначки, про наявність небезпечних вантажів у вагонах з комерційними несправностями, за запитом користувача видає на перегляд та друк аварійну картку.

Ведення книги реєстрації комерційних несправностей. АС ПКО забезпечує:

- формування записів електронної книги реєстрації комерційних несправностей за даними протоколу комерційного огляду;
- реєстрацію попутних актів загальної форми у електронній книзі реєстрації комерційних несправностей;
- друк аркушів книги реєстрації комерційних несправностей форми ГУ-98 з використанням даних електронної книги реєстрації комерційних несправностей;
- передачу записів електронної книги реєстрації комерційних несправностей на сервер застосувань рівня залізниці для зберігання та подальшого використання.

Формування та облік актів загальної форми. АС ПКО забезпечує:

- формування електронних актів загальної форми за даними протоколу комерційного огляду та електронних перевізних документів, з доданням до них відеоматеріалів стосовно проходження вагонів з комерційними несправностями;
- друк актів загальної форми ГУ-23;
- передачу електронних актів загальної форми на сервер застосувань рівня залізниці для зберігання та подальшого використання.

Формування та облік комерційних актів. АС ПКО забезпечує:

- формування електронних комерційних актів за даними протоколу комерційного огляду та електронних перевізних документів, а також, у разі необхідності – з використанням даних інших електронних актів (загальної форми та комерційних), що були складені за цією відправкою раніше, з доданням до них відеоматеріалів стосовно проходження вагонів з комерційними несправностями;
- заповнення за допомогою засобів ЕОТ бланків комерційних актів форми ГУ-22 та ІНУ-67;
- реєстрацію складених комерційних актів у електронній книзі обліку складених комерційних актів ГНУ-2, друк аркушів цієї книги;
- передачу електронних комерційних актів на сервер застосувань рівня залізниці для зберігання та подальшого використання.

Формування та друк оперативних повідомлень (тексту телеграм) по незбереженим вантажам та комерційним несправностям. АС ПКО забезпечує формування та друк оперативних повідомлень (тексту телеграм) по випадкам незбереженості вантажів та комерційним несправностям з використанням даних електронної книги реєстрації комерційних несправностей.

Складання та друк звітів про вагони з комерційними несправностями, виявленими на станції. АС ПКО забезпечує складання та друк звітів про вагони з комерційними

несправностями, виявленими на станції, форми КНО-5 з використанням даних електронної книги реєстрації комерційних несправностей.

Умови експлуатації АС ПКО. Задача повинна функціонувати в СКБД ORACLE в інформаційному середовищі - підсистемі сумісного функціонування Автоматизованої системи керування вантажними перевезеннями УЗ (ПСФ АСК ВП УЗ-Є) з використанням поїзної та вагонної моделей залізниці.

- проведення якісної відеозйомки при швидкості проходження поїзда не більше 25 км/год.
- автоматичне включення освітлення в умовах недостатньої видимості та режиму запису відеозображення при проходженні поїзду через зону зйомки і вимикання при закінченні зйомки.
- запис зображення при проходженні одночасно двох поїздів на суміжних коліях.

Відеокамери, що використовуються у комплексі та встановлюються на відкритому повітрі, повинні забезпечувати працездатність в будь-який час доби при змінах температури навколишнього середовища від –40 до +60ºС, при відносній вологість повітря до 100%, в умовах вібрації при проходженні рухомого складу та впливу електромагнітних полів, які створюються електричним струмом в контактній мережі, напругою, що складає 21-29 кВ. Обладнання, що встановлюється в приміщеннях, повинно цілодобово зберігати працездатність за наступних умов: діапазон зміни температур +18ºС...+25ºС; відносна вологість повітря при 25ºС: до 80%; вібрації при проходженні рухомого складу. Канали зв’язку повинні відповідати вимогам розробника програмного забезпечення та забезпечувати перегляд відеоінформації на встановлених місцях станції (відповідно до посадових обов’язків та технологічних функцій працівників ПКО).

Задача повинна функціонувати в режимі реального часу. Видача інформації працівнику ПКО повинна відбуватись одночасно з проходженням поїзда. Відеоінформація повинна надаватися працівникам ПКО у вигляді не менше 3-х проекцій зображення (вид зверху, зліва, справа) з можливістю одночасного перегляду на одному моніторі. Інформація про масу вантажу та відхилення центру маси повинна надаватися у вигляді протоколу зважування з переліком номерів вагонів. Інформація про порядок дій у разі виникнення аварійної ситуації з небезпечним вантажем надається на підставі аварійної картки.

Надання даних в автоматизованій системі комерційного огляду поїздів та вагонів повинно задовольняти наступним вимогам:

- забезпечення працівників ПКО при проходженні поїзда можливістю одночасного перегляду зображення з трьох камер, а при повторному перегляді – можливістю призупинення, збільшення та роздрукування цього зображення;

- при порушенні ТУ навантаження (вихід вантажу за габарит, перевантаження вагона понад його вантажопідйомність, зміщення центру маси понад допустимі норми) надання попередження працівникам ПКО ;

- після проходу поїзда – роздрукування протоколу результатів комерційного огляду (розходження номерів вагонів з натурним листом, невизначені номери, відсутність запірно-пломбувальних пристроїв, вагони з порушенням габариту, розходженням кількості місць на відкритому рухомому складі, зіставлення фактичної ваги брутто з вказаною в натурному листі тощо).

- ведення електронної книги ГУ-98, її формування, зберігання та друк;

- формування в автоматичному режимі акту загальної форми ГУ-23 за формою, встановленою Правилами, його зберігання і друку. Можливість, у разі необхідності, використання даних акту для інших документів, що стосуються перевезення за даною відправкою;

- у разі складання комерційного акта за результатами перевірки вантажу формування та зберігання електронного примірника акта за встановленою формою (в залежності від виду сполучення) з використанням наявної у базі даних інформації по складеним актам загальної форми за даною відправкою, а також заповнення за допомогою засобів ЕОТ бланків комерційних актів ГУ-22 та ІНУ-67;

- формування працівниками ПКО щомісячного та щоквартального звіту форми КНО-5 у електронному вигляді;

- формування оперативного повідомлення за результатами оформлення акту загальної форми, а також, у разі необхідності – за результатами перевірки вантажу у тих випадках, коли це передбачено Правилами;

- створення загальної бази даних по всім вихідним формам;

- формування інформації з аварійної картки на небезпечний вантаж.

Комерційний огляд з використанням АРМ ПКО може бути умовно розподіленим на наступні етапи:

1. Попереднє отримання інформації про стан вагону і вантажу, вагу вантажу (при оснащеності станції дислокації ПКО системою відеоспостереження та (або) тензометричними вагами);

2. Отримання та роздрукування відповідних вихідних форм для проведення комерційного огляду;

3. Фіксування часу початку комерційного огляду та безпосередньо комерційний огляд;

4. Фіксування результатів комерційного огляду та часу закінчення комерційного огляду;

5. Автоматизоване складання облікових форм по виявленим комерційним несправностям (актів загальної форми, актів про технічний стан вагона, рапортів та комерційних актів);

6. Отримання облікових та звітних форм по комерційним несправностям, що складаються на підставі актів загальної форми та комерційних актів (книга реєстрації комерційних несправностей, книга обліку складених комерційних актів, звіт про вагони з комерційними несправностями КНО-5).

Попереднє отримання інформації про стан вагону і вантажу, вагу вантажу може забезпечити тільки система відеоспостереження та тензометричні ваги.

Під час огляду поїздів з використанням системи відеоспостереження, працівник що працює з системою, відмічає вагони поїзду, які за його думкою можливо мають комерційні несправності. Ця ознака «проблемного» вагону фіксується в АРМ ПКО та використовується для роздрукування довідки для проведення комерційного огляду та для фіксування результатів комерційного огляду.

Перед початком комерційного огляду працівник ПКО роздруковує довідки по даним систем відеоспостереження та тензометричних ваг, що можуть бути отримані на цій станції (при необхідності переглядає відеоінформацію по проблемним вагонам). Якщо станція неоснащена ні однією з цих систем, то для проведення комерційного огляду роздруковуються розмічена ТГНЛ.

Після фіксування часу початку комерційного огляду виконується безпосередньо комерційний огляд. Після комерційного огляду засобами АРМ ПКО виконується фіксування результатів комерційного огляду. По вагонам поїзда проставляється відмітки по виявленим у них комерційним несправностям. Поїзд, по якому фіксуються комерційні несправності вагонів, вже повинен мати відмітки «проблемних» вагонів, що були зафіксовані системою відеоспостереження або тензометричними вагами. По результатам комерційного огляду, працівник ПКО може, як підтвердити ці ознаки, так і відмовитися від них. Також ознаки наявності комерційної несправності у вагонів, можуть бути проставлені і тим вагонам, які не

були зафіксовані як «проблемні» системою відео спостереження чи тензометричними вагами.

Послідовність виконання наступних операцій (фіксування часу закінчення комерційного огляду та автоматизоване складання актів загальної форми на вагони з комерційними несправностями) залежить від технології роботи станції. Спочатку може бути виконано фіксування часу закінчення комерційного огляду, а потім складання актів, або спочатку складаються акти, а потім фіксується час закінчення комерційного огляду.

Після закінчення комерційного огляду, робота з поїздом виконується по технології роботи конкретної станції (операції розформування поїзду, відправлення поїзду).

Поїзди, що були оглянуті за допомогою системи відео спостереження, повинні включатися у довідку результатів відео спостереження. Доступ до цієї довідки повинен бути забезпечений для рівнів ДН, залізниці та УЗ (ЦМ та ЦД). Інтерфейс цієї довідки повинен забезпечувати можливість перегляду відеоінформації та актів загальної форми по вагонам з комерційними несправностями.

Обробка з використанням АРМ ПКО поїздів, що прибули на станцію у розформування. По прибуттю поїзду на станцію в розформування черговий по станції пред'являє цей поїзд до комерційного огляду працівникам ПКО. При пред'явленні поїзду повідомляється парк та колія, куди прибув поїзд, час прибуття, номер та індекс поїзду.

Час початку комерційного огляду фіксується передачею засобами АРМ ПКО відповідного повідомлення. У повідомленні про початок комерційного огляду повинні міститися наступні дані: номер та індекс поїзду, дата і час початку огляду. Поїзди, які були оглянуті в комерційному відношенні, працівником за допомогою АРМ ПКО реєструються в електронному аналогу книги форми ГУ–98 (книга реєстрації комерційних несправностей).

Якщо комерційних несправностей не виявлено, то по закінченню комерційного огляду операція закінчення комерційного огляду фіксується передачею з АРМ ПКО відповідного повідомлення. Повідомлення про закінчення комерційного огляду повинно містити наступні дані: номер та індекс поїзду, дата і час закінчення огляду. По цьому повідомленню в книзі ГУ-98 фіксується комерційний огляд поїзду, в якому відсутні комерційні несправності.

Якщо під час комерційного огляду були виявленні вагони з комерційними несправностями, то працівник ПКО повідомляє про це маневровому диспетчеру (черговому по станції).

Засобами АРМ ПКО фіксуються вагони з виявленими комерційними несправностями.

Для цього поїзд, в якому були виявлені вагони з комерційними несправностями, викликається на АРМ ПКО. Вибір вагонів поїзду з комерційними несправностями виконується у вікні АРМ ПКО, яке має форму таблиці.

Таблиця 2 – Вікно АРМ ПКО

Номер поїзда ####	Ст. формування ####	№ составу ###	Ст. призначення ####
Парк № ##		Колія № ##	

№ п/п	№ Номер вагона	Ознака несправності	Дата та час виявлення несправності		Відмітка про усунення несправності	Коди	
						станції відправлення	ванта-жу
1	2	3	4	5	6	7	8

У шапці вікна автоматично виводяться номер та індекс поїзду, номер парку і номер колії прибуття. У табличній частині вікна виводиться список вагонів поїзда.

Нижче наведено порядок роботи з вікном реєстрації комерційних несправностей по вагонам поїзда.

В графах 1 та 2 – автоматично виводяться номери по порядку вагонів у поїзді і номери вагона.

В графі 3 – проставляється працівником ПКО ознака комерційної несправності. При функціонуванні на станції системи відеоспостереження та (або) тензометричних ваг, ця відмітка вже може бути поставлена за даними цих систем.

В графах 4 та 5 – вказується дата та час виявлення несправності (пропонується поточні дата та час, а працівник ПКО при необхідності може її відкоригувати).

В графі 6 відміток про усунення несправності працівником ПКО проставляється одне з нижченаведених значень:

- 0 – пропущено без усунення;
- 1 – усунуто без відчеплення вагона;
- 2 – усунуто з відчепленням вагона для перевірки;
- 3 – усунуто з відчеплення вагона для усунення;
- 4 – усунуто з відчепленням вагона для перевантаження.

Відмітки про усунення несправностей вибираються з НДІ АРМ ПКО.

Після вибору усіх вагонів поїзду з комерційними несправностями засобами АРМ ПКО формується повідомлення в АСК ВП УЗ-Є.

По прийому повідомлення про результати комерційного огляду на вагони поїзду з комерційними несправностями автоматично складаються в електронному вигляді заготовки актів загальної форми ГУ-23.

Якщо про вагон з виявленою комерційною несправністю вказано, що він потребує відчеплення від поїзда, то такому вагону в розміченій ТГНЛ автоматично проставляється призначення плану формування «вагон з комерційною несправністю з відчепленням».

Маневровий диспетчер (черговий по станції) при необхідності усунення комерційної несправності з відчепленням від поїзду дає команду оператору СТЦ про перестановку вагонів на колії, де виконується усунення несправностей. Оператор СТЦ переставляє вагон у заданий парк на задану колію з обов'язковим зазначенням причини відчеплення (по комерційній несправності).

Після вводу даних про комерційний огляд працівник ПКО вводить повідомлення про закінчення комерційного огляду. В повідомленні про закінчення комерційного огляду повинні міститися наступні дані: номер та індекс поїзду, дата і час закінчення огляду.

Після прийому повідомлення про закінчення комерційного огляду стає можливим прийом повідомлення про закінчення обробки поїзду по прибуттю.

До введення повідомлення про закінчення комерційного огляду введення результатів комерційного огляду можна робити кілька разів (для коригування, додавання і скасування).

Працівник ПКО, після введення оператором СТЦ повідомлення про закінчення обробки поїзда по прибуттю, немає можливості коригувати дані результатів комерційного огляду.

Без введення повідомлення про закінчення комерційного огляду оператор СТЦ не повинен мати можливість ввести повідомлення про закінчення обробки поїзда по прибуттю, запросити попередній чи кінцевий сортувальний листок, ввести повідомлення про перестановку вагонів.

На всі виявлені вагони з комерційною несправністю складається акт загальної форми ГУ-23, який підписується працівниками, що робили комерційний огляд. Акт загальної форми ГУ-23 складається в випадках, що передбачені Правилами складання актів. Акт загальної форми ГУ-23 складається в необхідній кількості екземплярів. Нумерація актів загальної форми для АРМ ПКО ведеться автоматично і окремо для кожного парку або вантажного району по закріпленому виділеному інтервалу в межах станції і не повинна повторюватися протягом року. Зміст несправностей в актах заповнюється відповідно змісту класифікаторів.

Система взаємодії клієнта та залізниці. Положення про взаємодію залізниці та клієнта. Взаємодія залізниці з клієнтами регламентуються Статутом залізниць України, здійснюється на підставі положень: Правил обслуговування залізничних під'їзних колій, Правил користування вагонами та контейнерами, договору про перевезення, Договорів про

експлуатацію під'їзних колій і договорів про подачу забирання вагонів та окремих додаткових угод (Kyrychenko H., Berdnychenko Yu., 2014).

При взаємодії залізниці з під'їзними коліями промислових підприємств враховуються наступні операції:

- інформування залізницею вантажовласника про надходження вагонів на його адресу;
- інформування вантажовласником залізниці про закінчення вантажних операцій вагонів;
- подавання – забирання вагонів для (після) вантажних операцій,
- користування вагонами залізниці промисловими підприємствами, клієнтами;
- маневрова робота локомотива залізниці на під'їзних коліях;
- затримки вагонів при подаванні забиранні вагонів, на підходах до станції призначення з вини вантажовласника;
- будь-які роботи за домовленістю та відповідно до Збірника тарифів

Розрахунки за подачу й забирання вагонів здійснюються на підставі Збірника тарифів за перевезення вантажів, розрахунки за користування вагонів здійснюється на підставі Правил користування вагонами та контейнерами.

Облік часу користування вагонами і контейнерами та нарахування плати за користування ними провадиться на станціях за Відомістю плати за користування вагонами форми ГУ-46. Облік подавання забирання вагонів, нарахування плати за ці види робіт здійснюється за Відомістю плати за подавання забирання вагонів форми ГУ-46а.

Документами оформлюються операції з взаємодії: повідомлення про подавання вагонів ф. ГУ-2; пам'ятки про подавання/забирання вагонів форми ГУ-45, що містить повідомлення про закінчення вантажних операцій з вагонами, акти про затримку вагонів на підходах до станції форми ГУ-23а, акти загальної форми про затримку вагонів з вини вантажовласника ГУ-23.

Для автоматизованого розрахунку документів з обліку роботи залізниці з під'їзною колією, відправником, клієнтом залізниці, з метою автоматизації технологічних процесів в системі взаємодії розроблена Інформаційна модель під'їзних колій, яка є підсистемою загальної системою АСК ВП УЗ-Є.

Мета створення системи – автоматизація технологічних процесів в системі взаємодії клієнта та залізниці, яка передбачає:

- автоматизовано провадити облік наявності і використання вагонів на під'їзній колії за номером вагона, з поділом часу знаходження на фактичний та час, за який нараховується плата за користування;

- автоматизувати нарахування плати за користування вагонами з урахуванням дії договорів про експлуатацію під'їзної колії та умов додаткових узгоджень;

- підвищити достовірність і своєчасність передачі інформації про операції з вагонами в модель під'їзних колій дорожнього рівня;

- виключити помилки при розрахунку плати за користування вагонами на під'їзній колії, підвищити достовірність розрахунків;

- створити архів операцій з вагоном на під'їзній колії.

Автоматизація технологічних процесів розрахунку часу, нарахування плати особливо ефективна на станціях із значними об'ємами вантажної роботи та складною технологією роботи – наявність декількох напрямків подавання – забирання вагонів (*Кириченко Г., Стрелко О., Бердниченко Ю., 2021*).

Облік часу користування вагонами здійснюється на підставі інформації з АРМ приймоздавальника про події з вагонами при подаванні та забиранні вагонів на (з) під'їзну колію, місця загального користування. Облік часу, який підлягає оплаті підприємством, залежить від умов договорів підприємства з залізницею, які містяться у системі паспортизації – АС паспортизації.

Інформаційна модель під'їзних колій утворюється та функціонує на базі 4 підсистем, взаємопов'язаних між собою, зокрема:

1. Єдина електрона картотека клієнтів – (нормативна інформація) – інформація про коди державної реєстрації підприємства, залізничні коди.

2. Система паспортизації під'їзних колій – (нормативна інформація), в яку вносяться технічні можливості вантажних фронтів та умови договорів і додаткових узгоджень, дані використовуються в розрахунках ГУ-46, ГУ-46а.

3. АРМ приймоздавальника – (вхідна інформація), здійснює підготовку та передачу даних пам'ятки ГУ-45, повідомлення про здійснення вантажної операції, одержує розраховану ГУ-46 з АСК ВП УЗ. В АРМі формуються пам'ятки, акти затримки вагонів з вини клієнта ф. ГУ-23, вводяться дані актів затримки на підходах до станцій ф. ГУ-23а, роздруковуються відомості плати фГУ-46, ф. ГУ-46а, підтримується логічний контроль з вагонною моделлю АСК ВП УЗ-Є. АРМ приймоздавальника це завершальна ланка в загальному процесі розрахунків з клієнтами за користування, подачу й забирання вагонів (*Kyrychenko H., Strelko O., Berdnychenko Y., Berdnychenko I., 2023*).

4. АСК ВП УЗ-Є – розрахунки відомостей плати (вихідна інформація) здійснюються на підставі даних договорів і фактичного часу подачі і забирання вагонів.

В АСК ВП УЗ-Є задіяні: модель розрахунків, вагонна модель, модель актів на затримку вагонів з вини залізниці, вантажовласника, в цій моделі обліковується час затримки на таможні, на кордоні, на шляху прямування у порти, при зайнятості фронтів тощо (*Kyrychenko H., Berdnychenko Yu., Strelko O., Shcherbyna R., 2021*).

Модель під'їзної колії «перекладає» інформацію про переміщення вагонів у інформацію про розрахунки на підставі договорів (*Kyrychenko H., Statyvka Y., Strelko O., Berdnychenko Y., 2021*).

Довідники, що використовуються в системі, аналогічні картотеки клієнтів, мають наступну структуру

Таблиця 3 – Структура довідників, що використовуються в системі

№	Поле	Ключ	Тип	Найменування поля БД
1	KOD	*	I(4)	Код підприємства
2	NAM		A(15)	Найменування підприємства
3	MNK		A(7)	Мнемокод
4	LSHT		I(8)	Лицьовий рахунок
5	NPP		I(3)	Номер повідомлення 1397

Таблиця 4 – Структура довідників кодів напрямків

№	Поле	Ключ	Тип	Найменування поля БД
1	PRED	*	I(4)	Код підприємства
2	KOD	*	I(2)	Код напрямку
3	NAME		A(24)	Найменування напрямку
4	KM		N	Кілометраж
5	NTABL		A(1)	Номер таблиці ставок
6	ZNIGKI		L	Ознака використання знижок
7	STAN		I(4)	Код станції

Напрямок подавання вагонів – обумовлене місце подачі вагонів. В АС ПЗ ПК по кожному напрямку подавання вагонів містяться дані про:

- приналежність локомотиву (залізниці, вантажовласника);

- відстань для нарахування збору за подачу / забирання вагонів;

- ознаку належності напрямку до групи напрямків для розрахунку середньозваженої відстані подачі / забирання вагонів.

Назва напрямку роздруковується в пам'ятках форми ГУ-45 на подавання/забирання вагонів в полі «Місце подавання/забирання».

Розмір фронту одночасної подачі вагонів – кількість вагонів, що було одночасно передано вантажовласникові по одній пам'ятці ГУ-45.

Розмір фронту одночасної обробки вагонів – кількість вагонів, що було одночасно оброблено. Характеризується одним часом повідомлення про закінчення вантажних операцій.

Модель під'їзної колії зв'язана з наступними моделями:

- вагонна модель - зв'язок здійснюється через номер вагону
- модель клієнт - зв'язок здійснюється через код клієнта
- відправочна модель - зв'язок здійснюється через код клієнта+код вантажу
- модель станції - зв'язок здійснюється через код станції
- поїзна модель – зв'язок здійснюється через ідентифікатор операції з потягом (код документа 050101.0.13.01.1.001);
- модель договорів - зв'язок здійснюється через код клієнта та договір;
- локомотивна модель - зв'язок здійснюється через ідентифікатор операції з локомотивом, який виконує маневрову роботу

Вихідні документи системи:

- облікові та звітні документи;
- довідково-аналітична система використання вагонів;
- довідково-аналітична система наявності вантажних фронтів та існуючих умов договорів.

Вихідні документи, розрахунок яких реалізований у системі:

- формування пам'ятки прийомоздавача про подачу і забирання вагонів форми ГУ-45. У рамках цієї задачі в моделі під'їзних колій при передачі інформації з АРМу прийомоздавача про подачу вагонів, забирання вагонів формується автоматизований документ форми ГУ-45 – пам'ятка про подавання-забирання вагонів;
- формування відомості плати за користування вагонами форми ГУ-46. У рамках цієї задачі визначається час знаходження вагонів на під'їзних коліях (при здійснені події – забиранні вагонів з підприємства) і на підставі цього, а так само на підставі актів про затримку вагонів форми ГУ-23 і ГУ-23а, діючих Правил користування вагонами та Статуту залізниці і відповідно до умов додаткової угоди під'їзної колії і залізниці нараховується плата за користування вагонами. При цьому формується документ форми ГУ-46;
- формування відомості плати за подачу і забирання вагонів. У рамках цієї системи здійснюється розрахунок відомості про подавання забирання вагонів локомотивом залізниці відомість плати ф. ГУ-46а . При наявності декількох станцій примикання і декількох напрямків автоматизована відомість начислення плати за подачу й забирання

вагонів складається по кожній відстані до станції примикання окремо. В цілому по станції за добу ці дані підсумовуються;

- формування, передача і коректування макета 1397. Для передачі даних про переміщення вагонів у вагону модель система формує макети 1397;

- формування звіту про нарахування плати за користування вагонами форми КОО-4. На підставі даних відомостей плати за користування вагонами автоматично формується відомість про нарахування плати за користування вагонами ф. КОО-4 за будь-який визначений період.

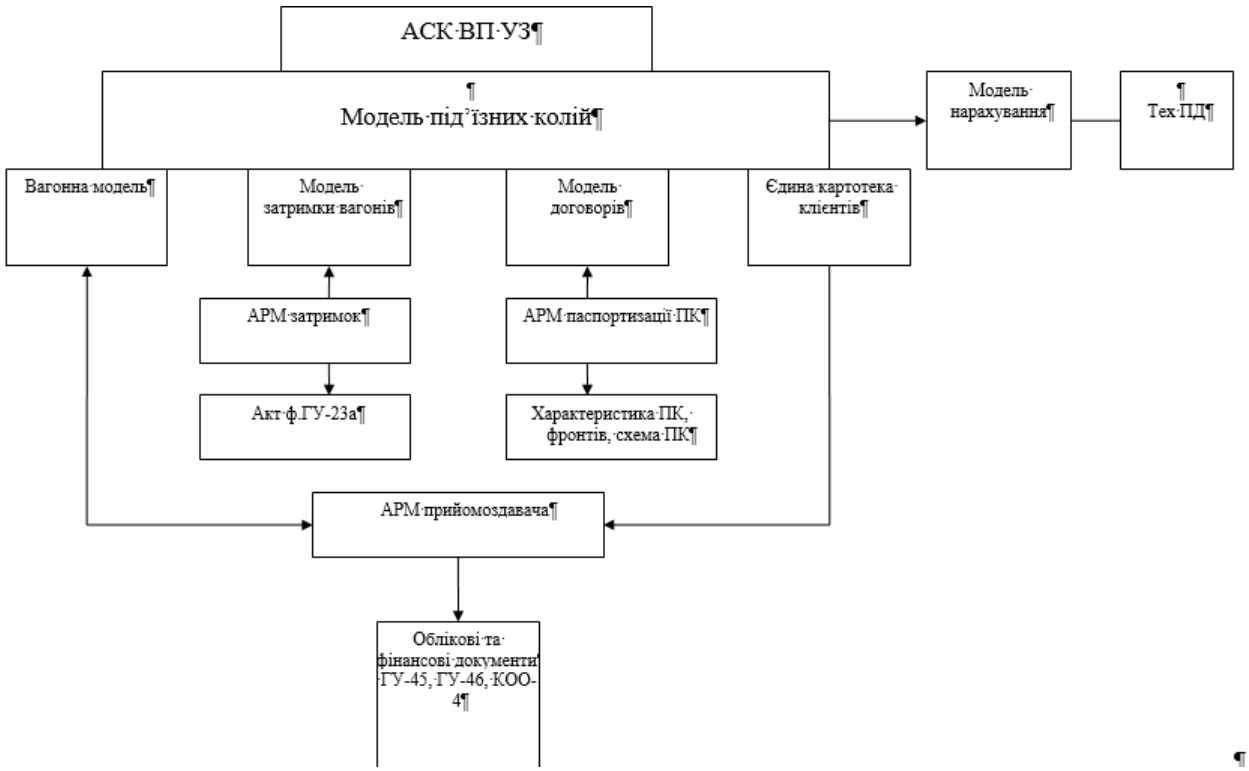


Рисунок 8 – Зв’язок моделі під’їзних колій з іншими моделями

Формування довідково – інформаційного матеріалу про використання вагонів на під'їзних коліях. У рамках задачі здійснюється пошук вагона за його номером, указується послідовність операцій із вагоном на під'їзній колії та видаються довідки про наявність вагонів, що знаходяться на промисловому підприємстві тривалий час

Довідково-аналітична система під’їзних колій. Довідково-аналітична система під’їзних колій призначена для забезпечення працівників станцій, ревізорів, керівництва структурних підрозділів залізниці, фахівців дирекції, залізниці, Укрзалізниці інформаційно-довідковою інформацією.

До аналітичної системи входить ряд задач, які є компонентами даної системи.

- задача «Формування довідок з інформацією по здійснених операціях по вагонах на під’їзній колії на підставі пам’яток ГУ-45 та за відомістю ГУ-46»;

- задача «Формування довідок про стан вагонної моделі під'їзної колії за всіма реквізитами пам'ятки на подачу, в т.ч. примітками, за визначений період часу»;
- задача «Формування довідок з інформацією по часу знаходження та користування вагонами, а також плати за користування на зазначений момент (запиту) не забраних вагонів (аналогічно «довгопростоюючим»)»;
- задача «Формування довідок з інформацією про подачу та забирання вагонів за родом рухомого складу за періодами доби та напрямками подачі – забирання»;
- задача «Формування довідок по нарахованих та стягнених платежах за користування вагонами по кожному підприємству, по станції, по ДН, по залізниці, по УЗ»;
- задача «Формування аналітичних довідок про переробну спроможність вантажних фронтів під'їзних колій підприємств на підставі даних АРМ паспортизації за реквізитами умов договорів та ЄТП»;
- задача «Формування довідок з обліку часу користування вагонами, нарахування плати за їх користування на під'їзних коліях»;
- задача «Формування довідок з контролю здійснення операцій «нараховано», «сплачено» за відомостями ф.ГУ-46 на забрані з під'їзної колії вагони».

Автоматизована система документообігу замовлень на перевезення вантажів та формування планів. Технологія взаємодії збутового і перевізного комплексів на всіх рівнях управління залишається актуальною в організації навантаження і відповідає ринку перевезень. Інтенсифікація експлуатаційної роботи вимагає організувати більш детальне планування перевезень і взаємний обмін інформацією між вантажовідправниками, вантажоодержувачами та залізницями.

Мета розробки підсистеми обліку оперативних заявок та контролю навантаження в АСК ВП УЗ-Є (надалі – обліку оперативних заявок) – реалізація в автоматизованій системі документообігу замовлень на перевезення вантажів та формування планів (АС Месплан) сумісної технології оперативного планування (уточненого зведеного замовлення) між всіма учасниками перевізного процесу з можливістю ведення електронної заявки на навантаження вантажів (ф.ГУ-11ВЦ) і її використання при контролі навантаження.

Задача «Розробка автоматизованої підсистеми обліку оперативних заявок та контролю навантаження в АСК ВП УЗ-Є» призначена для автоматизації оперативно-технологічної моделі планування перевезень, що забезпечує основу для вирішення задачі автопланування навантаження відповідно до замовлень Клієнта і контролю їх виконання та:

1. Формування електронної заявки на навантаження вантажів (далі електронна заявка або ф.ГУ-11ВЦ), в якій вантажовідправник / вантажоодержувач вказує дату і обсяги

навантаження у вагонах для кожної запланованої прогнозної дати навантаження, в строки дії плану перевезення і в межах узгоджених об'ємів плану перевезення;

2. Проведення логічного контролю наявності електронної заявки на навантаження вантажів при оформленні перевізних документів в АРМ ТВК;

3. Реалізації режиму жорсткого логічного контролю при оформленні перевізних документів на адресне відвантаження у суворій відповідності до обсягів та дат навантаження, вказаних в електронній заявці;

4. Ведення постійного моніторингу за ходом виконання планів перевезень з урахуванням фактичного щодобового навантаження;

5. Оперативного корегування вантажовідправником / вантажоодержувачем України ф.ГУ-11ВЦ залежно від експлуатаційної обстановки, що складається;

6. Виконання задачі підготовки пропозицій, підтримки ухвалення управлінських рішень при узгодженні додаткових планів, аналізування експлуатаційної обстановки і технологічної можливості перевантажувальних терміналів в частині термінів відвантаження і передачі потоків. Це дозволить ухвалити обґрунтоване рішення про можливість прийому нових (неузгоджених) заявок або про перенесення дат відвантаження по раніше прийнятих (узгоджених) заявках, щоб забезпечити рівномірне прибуття вагонів зі всіх станцій навантаження за призначенням і не допустити переповнювання складських місткостей або перевантажувальних механізмів за потужністю.

7. Поступовий перехід до сумісної технології оперативного планування замовлень на перевезення з розробкою можливості створення і ведення електронної заявки на навантаження вантажів (ф.ГУ-11ВЦ) як зі сторони вантажовідправника, так і зі сторони кінцевого одержувача вантажу на території України.

Використання даних з електронної заявки для проведення логічного контролю при оформленні перевізних документів, а також для автоформування в подальшому окремих даних електронної облікової картки Клієнта в частині плану і факту навантаження. Роботи проводяться в двох напрямках:

- розробка програмного забезпечення формування і ведення ф.ГУ-11ВЦ з прив'язкою до призначення плану перевезення, врахування змін плану (система автоматично відстежує додатково заявлені вагони планів);
- розробка програмного забезпечення реалізації логічного контролю дотримання електронної заявки на навантаження вантажів(ф.ГУ-11ВЦ) при оформленні перевізних документів.

Роботи по розробці програмного забезпечення ведення електронної заявки відвантаження, а також реалізації логічного контролю дотримання відповідності даних між перевізним документом і електронною заявкою проводяться в рамках програмного забезпечення АС Месплан в середовищі бази даних вузла АСК ВП УЗ-Є.

Вхідна інформація системи. Підсистема оперативного обліку заявок базується на фактичних даних: із наявних узгоджених заявок вантажовідправника на перевезення вантажів зі станцій навантаження (із заданим вантажем і заданому одержувачу) по кожному напрямку (розрахунковому елементу) перевезення масових вантажів. Вхідною інформацією є «варіант формування» й дані з електронної заявки на навантаження вантажів (ф.ГУ-11ВЦ), що вводить безпосередньо користувач системи АС Месплан після узгодження заявки на перевезення вантажу (форма ГУ-12) за допомогою АРМу АС Месплан. В АС Месплан користувачу, згідно з його статусом (вантажовідправник / вантажоодержувач), автоматично визначається режим доступ, або «варіант формування» форми ГУ-11ВЦ за датами, до яких належать:

1. «Заповнення вантажовідправником» - електронна заявка заповнюється вантажовідправником (проставляється кількість вагонів для певного календарного дня), починаючи від дати початку дії плану, для кожного призначення плану перевезення окремо.

2. «Заповнення вантажоодержувачем» - електронна заявка заповнюється вантажоодержувачем, починаючи від дати початку дії плану, для кожного призначення плану перевезення окремо.

Реквізитній склад даних для електронної заявки які передаються з АРМу в систему АС Месплан представлений в табл. 5.

Таблиця 5 – Реквізитній склад даних для електронної заявки які передаються з АРМу в систему АС Месплан

Назва атрибуту	Коментар
DAY	календарна дата відвантаження вантажу
K_COUNT	заявлена кількість вагонів на дату, без врахування попередніх днів
KOR_VAG (N)	скоригована кількість вагонів вантажовідправником/вантажоодержувачем
KOR_DAY (N)	дата коригування електронної заявки

Процеси АС настроюються відповідно до ведення і підтримки в актуальному стані галузевої нормативно - довідкової інформації із можливістю динамічно перенастроюватися при змінах технології роботи.

При реалізації даного програмного забезпечення використовуються наступні довідники / класифікатори:

- довідник експортних прикордонних стиків для визначення кодів пунктів здачі на водний транспорт, залізниці СНД, та в «треті країни»;
- єдиний електронний класифікатор клієнтів (ЄЕКК) для визначення по коду ЄДРПОУ вантажовідправника/вантажоодержувача, його ідентифікатору і чотирьохзначного коду;
- перелік вантажоодержувачів для яких розраховується відповідний «варіант формування» електронної заявки.

Дані для ведення переліку вантажоодержувачів для яких розраховується відповідний «варіант формування» електронної заявки надаються Головним управлінням перевезень. Формування переліку ведеться за допомогою АРМу Месплан.

Вихідна інформація. Підсистема АСК ВП УЗ-Є з автоматизації обліку оперативних заявок та контролю навантаження в результаті свого функціонування формує наступні довідки (вихідні форми):

1. ф.ГУ-11ВЦ для кожного окремого плану перевезень за призначенням, в т.ч. за скороченою формою;
2. зведеного плану навантажень за призначеннями: в порт, в «треті країни» по західним стиковим пунктам та в країни СНД і Балтії по міждержавним стиковим пунктам з залізницями СНД, в т.ч. за скороченою формою;
3. фрагмент облікової картки виконання плану перевезень.

Опис формування Електронної заявки для кожного окремого плану перевезень. Електронна заявка формується на підставі даних плану на перевезення з АС МЕСПЛАН за наступним реквізитним складом:

- відправник;
- залізниця відправлення;
- станція відправлення;
- номенклатурна група і номер плану;
- одержувач;
- код вантажу за ЄТСНВ (ГНВ);
- станція призначення/стиковий пункт;
- загальні узгоджені об’єми (вагони і тони розраховуються на основі інформації з ГУ-12)
- прогнозні узгоджені обсяги в вагонах для кожного дня дії плану – План (проставляє вантажоодержувач/вантажоотримувач);

- виконані обсяги навантаження для кожного дня дії плану – Факт (розраховується на основі інформації з ЕПД(п.4979)).

Довідка формується за запитом який поступає з робочого місця АРМу МЕСПЛАН. Дані будуть формуватися згідно прав доступу користувача до АС МЕСПЛАН. Дані, що видаються в вихідній формі, формуються на підставі плану перевезення, електронної заявки і накопичених даних про факт навантаження, що формуються з перевізних документів.

Опис формування зведеного календарного плану навантажень за призначеннями. Дана довідка формується на підставі узгоджених планів з АС МЕСПЛАН, даних з електронної заявки на навантаження вантажів і даних по фактичному навантаженню. Довідка формується за наступним реквізитним складом:

- відправник;
- залізниця відправлення;
- станція відправлення;
- одержувач;
- номенклатурна група / код вантажу за ЄТСНВ;
- станція призначення / стиковий пункт;
- перелік узгоджених планів / узгоджені об`єми (вагони і тони);
- сукупні прогнозні обсяги (узгоджені) з електронних заявок (кількість вагонів) для кожного дня дії плану - План;
- сукупні виконані обсяги навантаження для кожного дня дії плану – Факт.

Довідка формується за запитом який поступає з робочого місця АРМу МЕСПЛАН.

Дані в довідці можуть бути відфільтровані по залізниці відправлення, станції відправлення, вантажовідправнику, вантажоодержувачу, номенклатурній групі вантажу, типу стика виходу (море-суша) або станції призначення. Дані будуть формуватися згідно прав доступу користувача до АС МЕСПЛАН.

Опис формування фрагменту облікової картки виконання плану перевезень. Фрагмент облікової картки виконання плану перевезень формується на підставі даних електронної заявки з АС МЕСПЛАНу і даних про фактичне навантаження, що формуються в АРМ ТВК. При цьому в обліковій картці заповнюються графи 1-3 (число і планові об’єми в вагонах і тонах), 5-6 (завантажені об’єми в вагонах і тонах), 10-15 (розподіл по залізницях призначення). Довідка формується за запитом який поступає з робочого місця АРМ МЕСПЛАН .

Опис алгоритму побудови підсистеми обліку оперативних заявок та контролю навантаження в АСК ВП УЗ-Є. Підсистема АСК ВП УЗ-Є з автоматизації обліку

оперативних заявок та контролю навантаження призначена для ведення форми ГУ-11ВЦ в межах кожного призначення плану перевезення і використання даних електронної заявки в підсистемі контролю при оформленні перевізних документів.

Опис алгоритму формування і введення даних у ф.ГУ-11ВЦ для кожного окремого плану перевезень по призначеннях. Електронна заявка формується для кожного призначення плану перевезення. Під електронною заявкою будемо розуміти розбивку узгоджених об'ємів призначення плану перевезення у вагонах по календарних датах в межах строків дії плану.

При цьому кількість вагонів в електронній заявці заноситься з врахуванням недовантаження (при його наявності) за попередні дні і без врахування загальних узгоджених об'ємів. Таким чином сумарна кількість вагонів в електронній заявці (план) за всі дні дії плану може перевищувати загальну узгоджену кількість вагонів за даним призначенням.

З електронною заявкою можуть проводитись наступні операції: формування електронної заявки та корегування електронної заявки.

Опис алгоритму проведення операції формування електронної заявки. Створення електронної заявки проводиться засобами Арму АС Месплан після проведення операції узгодження заявки на перевезення для всіх видів планів (основний і додатковий). В процесі виконання операції «узгодження» для кожного призначення плану перевезення автоматично розраховується «варіант формування» електронної заявки. Розрахунок проводиться згідно наступних критеріїв:

1. Варіант формування електронної заявки приймає значення «заповнення вантажовідправником» в разі, якщо план на перевезення має вантажоодержувача не зазначеного в Переліку і вид перевезення «не експорт».

2. Варіант формування електронної заявки приймає значення «заповнення вантажоодержувачем» у разі узгодження перевезення:

- зі станцій України в «треті країни» чи країни СНД через вихідні припортові станції УЗ;
- зі станцій України в «треті країни» через сухопутні західні переходи УЗ;
- зі станцій України у адресному внутрішньому сполучення, для заданого окремого переліку вантажоодержувачів України.

В разі виникнення суперечки між «варіантами формування» електронної заявки, пріоритетність набуває варіант «заповнення вантажоодержувачем».

Ручна зміна «варіанту формування» в процесі корегування плану на перевезення зі сторони користувачів АС Месплан неможлива.

Після проведення операції узгодження плану на перевезення вантажовідправнику / вантажоодержувачу дозволяється формувати електронну заявку. Можливість формування електронної заявки надається засобами АРМу Месплан залежно від статусу абонента і розрахованого «варіанту формування» електронної заявки. Вантажовідправник або вантажоодержувач у відповідності з технологічними правами здійснює безперервне планування навантаження в електронному вигляді через АС Месплан з зазначенням кількості вагонів по календарних датах (електронна заявка).

При розрахованому «варіанті формування» електронної заявки в значенні «заповнення вантажовідправником», відправник безпосередньо чи особа за його дорученням, вручну заповнює дати і об'єми навантаження у вагонах (прогнозні дані). Дозволяється формувати електронну заявку в проміжку від поточної дати до кінцевої дати дії плану (закінчення планового місяця).

При розрахованому «варіанті формування» електронної заявки в значенні «заповнення вантажоодержувачем», ф.ГУ-11ВЦ формує безпосередньо одержувач вантажу за допомогою АРМ Месплан за схемою «дати і обсяги навантаження». Контроль переліку дат проводиться аналогічно до варіанту «заповнення вантажовідправником». У разі використання такого варіанту формування календаря, вантажовідправник не проводить розбиття заявлених об'ємів перевезення по датах навантаження (без права збереження даних). Користувач забезпечує своєчасне внесення змін (корегувань) в електронну заявку.

Опис алгоритму оперативного корегування електронної заявки. Подальша взаємодія збутового і перевізного комплексів в частині виконання електронної заявки будується на технології оперативного корегування електронної заявки (її подальше уточнення). В цьому випадку умови прав формування електронної заявки і умови прав її корегування повинні бути тотожними. Форма ГУ-11ВЦ уточнюється щодобово в оперативному режимі у відповідності з технологічними правами формування електронної заявки Клієнтом, але не пізніше, ніж за 24 години до початку залізничної доби, в якій планується проводити навантаження. Допускається корегування електронної заявки за принципом «сьогодні на сьогодні» або «сьогодні на завтра» виключно у бік збільшення об`ємів. Корегування електронної заявки за принципом «сьогодні на вчора» не допускається.

Корегування електронної заявки за принципом «сьогодні на сьогодні» допускається.

Опис перевірки логічного контролю дотримання електронної заявки на навантаження вантажів при оформленні перевізних документів. Задача логічного контролю дотримання електронної заявки на навантаження вантажів при оформленні перевізних документів розробляється в межах АС Месплан. Задача реалізується в середовищі бази даних вузла АСК

ВП УЗ-Є. Програмна реалізація задачі логічного контролю передбачає використання загальних правил побудови задач логічного контролю, прийнятих в АСК ВП УЗ-Є.

Логічний контроль здійснюється при передачі п.4979 в АСК ВП УЗ. Для програмної реалізації задачі використовується механізм співвідношення перевізного документу до плану перевезення. Опис механізму наведений в документі 410201.0.18.01.0.001 «Розробка технології та програмного забезпечення підсистеми АСК ВП УЗ-Є з автоматизованого контролю наявності планів на перевезення вагонів (форма ГУ-12). Методичні матеріали».

В разі, якщо знайдений план, що задовольняє параметрам перевізного документу і він має невиконані об'єми для проведення операції навантаження, то проводиться додаткова перевірка згідно наступного алгоритму:

1. Перевіряється наявність в призначенні розрахованого параметра «варіант формування» електронної заявки;
2. В разі відсутності вказаного параметра додаткова перевірка припиняється, логічний контроль завершується без фіксації помилки;
3. В разі наявності вказаного параметра відбувається пошук заповненої електронної заявки на дату оформлення перевізного документу;
4. В разі відсутності електронної заявки на дату оформлення перевізного документу, або в разі наявності електронної заявки з кількістю замовлених вагонів меншою за накопичені дані про фактичне навантаження вагонів для календарної доби оформлення перевізного документу, фіксується помилка і логічний контроль припиняється;
5. В разі наявності електронної заявки на дату оформлення перевізного документу з кількістю замовлених вагонів більшою або рівною накопиченим даним про фактичне навантаження вагонів для календарної доби оформлення перевізного документа, логічний контроль завершується.

У випадку, коли дані з п.4979 не пройшли логконтроль, видається одна з наступних помилок:

- відсутня електронна заявка;
- кількість вагонів для дати навантаження більша від замовленої кількості вагонів згідно ф.ГУ-11ВЦ.

Автоматизовані технології логістичного центру залізниці. Як нам відомо однією з головних цілей функціонування залізниці є надання транспортної послуги вантажовідправнику. Зараз управління вантажними перевезеннями на залізничному транспорті функціонує в інших умовах ніж два – три десятка років тому. Якщо раніше на ринку транспортних послуг умови диктував потужний виробник державної власності і

задача залізниці складалась у переробці значних обсягів вантажу, який він відправляв, то зараз ситуація змінюється - головною задачею залізниці постає задача надання транспортної послуги будь якому клієнту – крім крупного - середньому, разовому. Причому послуга повинна бути - якісною. Існуючи умови конкуренції на ринку транспортних перевезень диктують вимоги підвищення якості надання послуги.

У центрі вантажного транспорту стає клієнт, його потреби та вимоги, на які повинні реагувати пропозиції залізниці.

Також обробка транзитних вантажопотоків, що складають значну, прибуткову частину у структурі перевезень, потребує теж нових форм організації транспортного обслуговування.

Обслуговування на основі логістичних підходів - надання повного та якісного спектру транспортних послуг. До логістичних принципів відноситься:

- раціональне управління організацією перевезення,
- комплексність обслуговування,
- використання автоматичних систем для виконання складських, навантажувально-розвантажувальних операцій у портах;
- використання математичного апарату для використання систем підтримки прийняття рішення,
- виконання вимог клієнта для збереження конкурентоспроможності залізниці,
- використання автоматизованих технологій для оцінки якості процесу, інформованості про здійснення операцій;

Однією з важливих складових логістичного забезпечення є інформаційне забезпечення процесу перевезення, що реалізується за допомогою автоматизованих систем і дозволяє спростити спілкування клієнта з залізницею (*Кириченко Г., Цейтлін С., 2021*).

Як ми раніше відмітили, вимоги часу змінили порядок відношень між клієнтом і залізницею (*Кириченко Г.І., Цейтлін С.Ю., Чередниченко О., 2021*). Традиційна технологія оформлення перевезення вантажу на залізничній станції відправлення, коли клієнт повинен декілька разів звертатися в різні підрозділи від товарної контори залізничної станції до управління залізниці або навіть до Державної адміністрації залізничного транспорту України не відповідала сучасним вимогам ринку транспортних послуг.

З 2006 виникають та формуються нові методи роботи, нові «інструменти» для реалізації логістичного забезпечення на залізниці:

- підвищення зручності при оформленні перевезень, а саме створення єдиних ТехПД, які зараз використовують єдині картотеки клієнтів, та працюють за принципами єдиного

сальдо на особистому рахунку - підвищення рівня прозорості при розрахунках за обслуговування клієнтів,

- впровадження електронного документообігу з вантажовласниками

- оформлення документів за допомогою автоматизованих систем: перевізні документи; складати пам'ятки на подавання – забирання вагонів; розраховувати відомості плати за користування вагонами; розраховувати відомості плати за подавання – забирання вагонів; перейти до впровадження електронного перевізного документу у вантажних перевезеннях, надання оперативного замовлення (на 2-3 доби) на перевезення.

Продовження впровадження цих методів є - надання повного спектру логістичних послуг. Стримуючим фактором роботи в цьому напрямку є відсутність логістичної інфраструктури залізниці.

Відсутність зараз логістичної інфраструктури обумовлюється:

- відсутністю транспортного конвеєру в частині постачань, що відповідають за початкові – кінцеві операції термінальних комплексів, в т. ч. мультимодальних;

- відсутністю підсистеми інформаційної підтримки прийняття рішення;

- відсутністю інструменту, що забезпечує оптимальну взаємодію вантажовласників, залізниці, суміжних видів транспорту, експедиторів, операторів - власників вагонного парку, інших учасників ланцюга постачань з точки зору покращення використання інфраструктури та рухомого складу;

- виникненням реальних втрат, пов'язаних з збільшенням терміну доставки, простоями вагонів у «кинутих поїздах» на підходах до портів, прикордонних переходів та промислових підприємств.

Функціонування логістичного центру залізниці пов'язано з системним підходом до вирішення задач складання графіків доставки вантажів, маркетингу, прогнозування, виявлення «вузьких місць» на підставі аналізу потреб клієнтів та наявних можливостей залізниці, розробки методик та пропозицій розвитку (в чому числі з розвитку термінальної інфраструктури).

Це дозволить задовольнити актуальні вимоги клієнта:

- необхідність доставки вантажів «точно в строк»; «від дверей до дверей»; гнучкого рівня транспортного обслуговування; митного обслуговування при експортно-імпортних перевезеннях; супроводження вантажу.

- зручність пред'явлення вантажу до перевезення; розташування пунктів навантаження; отримання вантажу у пунктах призначення; інформаційного обслуговування;

- забезпечить надійність та регулярність перевезень; їх безпеку та збереження.

Діяльність центру також дозволить:

- оптимізувати вартість перевезення та перевантажувальних операцій на шляху прямування;

- інформувати про тарифи та умови на перевезення; про місцезнаходження і стан вантажу під час перевезення.

- надасть додаткові сервісних послуг; в т.ч. необхідну транспортну тару та раціональну технологію в пунктах перевалки та перетину міждержавного кордону.

Виходячи з функцій центру, передбачається організація логістичної інфраструктури за схемою, структура якого реалізує:

- розрахунки в Єдиному центрі при їх оформленні через комерційного агента центру та прозорості при нарахуваннях платежів за перевезення;

- контроль за перевезеннями – у Диспетчерській службі, яка співпрацює з Головними управліннями УЗ та приймає замовлення від клієнтів на всі види послуг і координує роботу з клієнтами;

- функціонування всієї структури відбувається в єдиному інформаційному середовище.

Єдиний розрахунковий центр планується організувати на базі єдиних ТехПД та розрахункового центру за транзитні перевезення.

Автоматизоване робоче місце комерційного агента центру передбачено створити як інтегроване на базі АРМ ТВК та АРМ ПЗ (*Kyrychenko H., Statyvka Y., Strelko O., Berdnychenko Y., Nesterenko H., 2018*).

Ефективність логістичного ланцюга значно підвищиться з використанням електронного документообігу у взаємовідношеннях з клієнтами.

Впровадженню електронного перевізного документу сприяє розпорядження КМУ про затвердження «плану заходів із запровадження електронного документообігу, пов'язаного з перевезенням вантажів залізничним транспортом».

Для більш зручної підготовки документів та зменшення часу їх оформлення Главком підготовлені зміни до Правил перевезень, які передбачають оформлення всіх видів перевезень за єдиною формою та на одній стороні.

Організація логістичної інфраструктури передбачає забезпечення прозорості при нарахуваннях платежів за перевезення, для цього у роботі з вантажовідправниками необхідно запровадити Інтернет-технології: підписанню договорів, при оформлення заявок, перевізних документів, узгодженню облікових, підписанню фінансових документів засобами Веб-офісу.

Відповідно плану заходів із запровадження електронного документообігу за Постановою КМУ на визначеному полігоні Донецької залізниці апробовано оформлення та передача електронного документу за цифровим підписом.

Створення та запровадження логістичної інфраструктури залізниці, забезпечить надання послуги, якість якої диктують існуючи умови конкуренції на ринку транспортних перевезень.

Таким чином, логістичне забезпечення при виконанні транспортних послуг передбачає:

- створення єдиного логістичного центру залізничного транспорту;
- розробку методів складання (та узгодження сторонами) технології конкретного перевезення вантажу та контроль графіку його виконання;
- інтелектуалізацію процесів управління перевезеннями вантажів на підставі створення автоматизованих систем підтримки прийняття рішення для оптимізації перевезень вантажів.

Ці складові єдиного інформаційного простору залізниці – інтегрованої автоматизованої системи залізниці.

Функціонування логістичного центру залізниці пов’язано з вирішенням задач складання графіків доставки вантажів, маркетингу, прогнозування.

Використання інноваційних технологій на базі вдосконалення технологічних процесів обробки вагонів та вантажів дозволить оптимізувати перевізний процес, продовжити його до «дверей клієнта» та перейти до прозорості нарахувань у єдиному розрахунковому центрі. Для цього існуючий склад інформаційного середовища необхідно доповнити даними про транспортні процеси, інформаційними технологіями та автоматизованими системами:

- прогнозування та контроль дотримання графіків доставки вантажів окремими учасниками перевезень;
- прогнозування маркетингових умов – прогнозування ринку транспортних послуг з урахуванням прогнозу обсягів перевезень, існуючого ринку власників рухомого складу та експедиторських послуг;
- визначення кількісних критеріїв оцінки ефективності окремого перевезення та процесу перевезень вантажів;
- моделювання та оптимізації процесу доставки вантажів;
- система прийняття рішення щодо станції затримки поїзду на підходах до станції призначення з вини вантажовласника;

- інформаційна система для організації процесів ввезення, складування, вивезення вантажів дистанціями МЧ, вибору доцільної транспортної тари, вибору місця розташування вантажу на складі, здійснення контролю обсягів вантажів, визначення місця розташування складів;

- єдина система обробки вагонів та вантажів на прикордонних станціях;

- оптимізація місцевої роботи в залізничному вузлі.

Існуюче інформаційне забезпечення необхідно вдосконалити наступним:

- організацією єдиної картотеки клієнтів УЗ;
- обробкою перевізних документів на транзитні вантажі та внутрішні здійснюється в єдиному розрахунковому центрі УЗ;
- впровадженням технології отримання даних про час здійснення вантажних операції та стан вагону по вантажних фронтах промислових підприємств;
- впровадженням технології обробки даних про стан придатності під навантаження вагону певним вантажем та про згоду відправника на подавання під навантаження вагону;
- автоматизованим, з участю клієнта, складанням облікової картки із застосуванням Веб-технологій;
- узгодженням відомостей плати за користування вагонами, подаванням – забиранням вагонів, пам'яток про подавання-забирання із застосуванням Веб-технологій.
- розрахунком єдиного сальдо по клієнту.

Висновки. Наразі автоматизована система залізниці є інформаційним середовищем, де інтегровані всі події з основними об'єктами управління - вагоном та вантажем. Існуючи взаємозв'язків між складовими інформаційного простору забезпечують послідовність виконання технологічних операцій з об'єктами управління, внаслідок чого база даних системи є потужним комплексом для аналізу експлуатаційних подій та розрахунку фінансових та звітних документів. Унікальність АСК ВП УЗ-Є спричиняє логіка послідовності виконання операцій, що дозволяє на підставі даних перевізного документу, який оформлює відправник, та подій з вагоном та вантажем формувати всі фінансові та облікові документи, включно до податкових накладних. Структура системи дозволяє зберігати принцип модульності та відкритості, що є важливим при нарощуванні функцій системи. Необхідний розвиток автоматизації залізниці пов'язаний з розробкою інтелектуальних технологій для управління експлуатаційною роботою, що включає функції прогнозу, вибору оптимального управлінського рішення та управління технологіями.

References:

Науменко П. П., Миненко В. Д., Землянов В. Б. АСК ВП УЗ як основа інтеграції автоматизованих систем управління вантажними перевезеннями залізничного транспорту України». URL: https://stp.diit.edu.ua/article/download/17551/15290

Башлаєв В. К., Цейтлін С. Ю., Великодний В. В. Про створення сітьової автоматизованої системи управління вантажними перевезеннями України. Вісник Дніпропетровського національного університету залізничного транспорту ім. акад. В. Лазаряна. 2007. Вип. 17. С. 18-21.

Цейтлін С. Ю., Коваленко Л. А., Николенко М. В. Створення електронного архіву облікових і звітних форм даних в АСК ВП УЗ–Є. Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості та освіті: тези IX міжнар. наук.-практ. конф. Дніпропетровськ, 2015. С. 41.

Цейтлін С. Ю., Подоляк С. В., Василишин І. Д. Передумови створення аналітичної системи. Створення централізованої бази даних фінансово-економічних систем. Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості та освіті: тези IX міжнар. наук.-практ. конф. Дніпропетровськ, 2015. С. 97.

Кириченко Г. І. Методика створення інтелектуальної автоматизованої системи управління доставкою вантажів на залізниці. Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту. 2017. № 2 (68). С. 46-56.

Кириченко Г.І. Методологія підвищення ефективності експлуатації засобів транспорту шляхом вдосконалення науково-обґрунтованої стратегії управління технологічними процесами: автореф. дис… доктора техн. наук. 05.22.20 – експлуатація та ремонт засобів транспорту. Київ, 2021. 40 с.

Кириченко Г.І., Стрелко О.Г., Бердниченко Ю.А., Макарова О.О. Організація роботи сортувальної станції в умовах автоматизації. Збірних наукових праць Державного економіко – технологічного університету транспорту. Серія «Транспортні системи і технології», Вип.23. Київ: ДЕТУТ, 2013. С.150 -154.

Kyrychenko H., Strelko O., Berdnychenko Yu., Hurinchuk S. Automation of Work Processes at Ukrainian Sorting Stations. International Journal of Engineering & Technology. 2018. №7 (2.23). P. 516–518. https://doi.org/10.14419/ijet.v7i2.23.15346

Кириченко Г.І., Бердниченко Ю.А. Складові інформаційної моделі перевізного процесу вантажних перевезень залізничного транспорту. Інформаційно-керуючі системи на залізничному транспорті. 2021. Том 26 № 3. С. 12-17. https://doi.org/10.18664/ikszt.v26i3.240455

Кириченко Г. І., Габа В. В., Висоцька Г. С. Автоматизований облік часу затримки вагонів та вантажів на підходах до станцій призначення. Залізничний транспорт України. 2011. № 1. С. 30-32.

Kyrychenko H.. Berdnychenko Yu. Elektronische Abfertigung der Güterbeförderungen in der Ukraine. Збірних наукових праць Державного економіко – технологічного університету транспорту. Серія «Транспортні системи і технології», Вип.24. Київ: ДЕТУТ, 2014. С. 237-239.

Кириченко Г.І., Стрелко О.Г., Бердниченко Ю.А. Вдосконалення технології розрахунку показників експлуатаційної роботи з використанням автоматизованої системи. Сучасні технології в машинобудуванні та транспорті. 2021. Том 2 № 17 С. 81-88 https://doi.org/10.36910/automash.v2i17.637

Kyrychenko H., Strelko O., Berdnychenko Y., Berdnychenko I. Development of Automation of Operational Work of Railway Stations of Ukraine. 2023 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Kyiv, Ukraine, 2023, pp. 71-75. https://doi.org/10.1109/UkrMiCo61577.2023.10380415

Kyrychenko H., Berdnychenko Yu., Strelko O., Shcherbyna R.. Application of the Automated System at the Change of Technology of Work of Reference Stations on the Railway. Transport means 2021 Sustainability: Research and Solutions. Proceedings of the 25th international scientific conference. 2021. Part II. October 06-08. P. 782-786.

Kyrychenko H., Statyvka Y., Strelko O., Berdnychenko Y. Control of technological processes using a fuzzy controller of the system for management of cargo delivery by railway. Acta Scientiarum Polonorum Administratio Locorum. 2021. №20(3). P. 241–251. https://doi.org/10.31648/aspal.6808

Кириченко Г.І., Цейтлін С.Ю. Що гальмує євроінтеграцію залізничної логістики України. Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості і освіті: Тези XV Міжнародної науково-практичної конференції (Дніпро, 16-17 грудня 2021 р.). Д .: ДІІТ, 2021. С. 31-32.
Кириченко Г.І., Цейтлін С.Ю., Чередниченк О. С. Взаємодія інформаційних систем учасників залізничних перевезень. Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості і освіті: Тези XV Міжнародної науково-практичної конференції (Дніпро, 16-17 грудня 2021 р.). Д .: ДІІТ, 2021. С. 33-34.
Kyrychenko H., Statyvka Y., Strelko O., Berdnychenko Y., Nesterenko, H. Assessment of Cargo Delivery Quality Using Fuzzy Set Apparatus. International Journal of Engineering & Technology, 2018. № 7(4.3). P. 262-265.

DOI 10.5281/zenodo.10822001

UDC 629.43

CHAPTER 17.
RESEARCH AND DEVELOPMENT OF A MULTIFUNCTIONAL SYSTEM FOR AUTOMATION OF ELECTROMECHANICAL EQUIPMENT OF URBAN ELECTRIC TRANSPORT

Serhii YESAULOV

Candidate of Technical Sciences, Associate Professor,

Associate Professo of the Department of Electric Transport,

O.M.Beketov National University of Urban Economy in Kharkiv,

(17, Marshal Bazhanov Street, Kharkiv, 61002, Ukraine)

serhii.yesaulov@kname.edu.ua

https://orcid.org/0009-0006-3274-716X

Olha BABICHEVA

Candidate of Technical Sciences, Associate Professor,

Associate Professor of the Department of Electric Transport,

O.M.Beketov National University of Urban Economy in Kharkiv,

(17, Marshal Bazhanov Street, Kharkiv, 61002, Ukraine)

olga.babicheva@kname.edu.ua

https://orcid.org/0009-0003-1294-2740

Annotation. Engineering techniques and options for developing components of a thermal process control system in existing electromechanical equipment in urban electric transport are considered. The results of a study of heating of different parts of equipment during the implementation of the operating cycle are presented. Studies have been carried out on a device with multiple temperature sensors and a visual spectrograph for monitoring thermal events with stochastic properties. The presented illustrations of the temperature control device interface confirm the possibility of using it in remote means of monitoring and diagnosing possible equipment malfunctions based on the intensity of heat generation by its individual parts. Using models of electronic means, an analysis and synthesis of the components of the local automation system was carried out, which made it possible to propose a version of a system for thermal stabilization of heating of electromechanical equipment based on a classic PID controller and a fuzzy algorithm block for changing the settings of the regulator settings.

Key words: sensor, control, thermal process, regulation, modeling, diagnostics, automation, electromechanics, control system, fuzzy algorithm.

ДОСЛІДЖЕННЯ І РОЗРОБКА БАГАТОФУНКЦІОНАЛЬНОЇ СИСТЕМИ АВТОМАТИКИ ЕЛЕКТРОМЕХАНІЧНОГО ОБЛАДНАННЯ МІСЬКОГО ЕЛЕКТРОТРАНСПОРТУ

Анотація. Розглянуто інженерні прийоми та варіанти розробки компонентів системи управління тепловими подіями в діючому електромеханічному обладнанні на міському електротранспорті. Наводяться результати дослідження нагрівання різних частин устаткування під час реалізації робочого циклу. Виконано дослідження пристрою з кількома датчиками температури та візуальним спектрографом для контролю теплових подій зі стохастичними властивостями. Представлені ілюстрації інтерфейсу пристрою контролю температури підтверджують можливість його застосування в дистанційних засобах контролю та діагностики можливих несправностей обладнання за інтенсивністю генерацією тепла окремими частинами його. За допомогою моделюючих електронних засобів виконано аналіз та синтез компонентів локальної системи автоматики, що дозволило запропонувати варіант системи теплової стабілізації нагріву електромеханічного обладнання виконаної на базі класичного ПІД-контролера та блоку нечіткого алгоритму зміни налаштування уставок регулятора.

Ключові слова: датчик, контроль, тепловий процес, регулювання, моделювання, діагностика, автоматика, електромеханіка, система управління, нечіткій алгоритм.

Вступ. На міському електротранспорті (МЕТ) сучасна електронна техніка дозволяє синтезувати бортові пристрої для оперативного контролю технологічних величин, діагностики справності обладнання та автоматичного керування різними параметрами. Застосування мікроелектронної техніки покращує умови праці, підвищує достовірність оцінки технічного стану обладнання, сприяє зниженню витрат ресурсів під час експлуатації та обслуговування рухомих одиниць (РО). Дослідження та розробка нових технічних рішень для рухомого транспорту засновано на сучасних технологіях в галузі електроніки та телекомунікацій, які є **актуальними** та важливими.

Метою дослідження була розробка пристрою вимірювання температури із заданою точністю, що дозволяє вдосконалювати вбудовані системи діагностики та управління тепловими процесами, що супроводжують експлуатацію електромеханічного обладнання (ЕМО) при змінних навантаженнях.

Для реалізації поставленої мети вирішувалися такі **завдання:**

– аналіз існуючих засобів безпечного контролю, діагностики та управління об’єктами ЕМО у діючому рухомому транспорті;

– дослідження та розробка пристрою контролю для теплового діагностування справності компонентів ЕМО у реальному часі;

– дослідження та розробка керуючого пристрою тепловими режимами експлуатації частин ЕМО.

Об’єктом дослідження були окремі частини ЕМО, теплові процеси яких потребували підвищення точності вимірювань температури, можливості реалізації теплової діагностики справності окремих дорогих компонентів та вдосконалення системи теплової стабілізації умов експлуатації транспортного силового обладнання.

На основі стаціонарних засобів вимірювання та методик для пошуку несправностей за фактом відмови, сучасним діагностичним пристроям доступна реалізація алгоритмів визначення багатьох причин, що виявляються при робочих навантаженнях, що передують поломкам окремих частин електромеханічного обладнання *(Квасніков В. П., Квашук Д. М., Катаєва М. О., 2021)*.

Прогнозування неполадок у тягових електроприводах (ТЕП) допомагає визначати перспективу можливого зношування різних компонентів обладнання. У більшості випадків поломки та відмови є наслідком поступового накопичення пошкоджень, поступового старіння та зношування працюючих окремих частин *(Афанасов А. М., 2013)*. При цьому, наприклад, робота тягового електродвигуна можлива за наявності в ньому деяких дефектів (коротке замикання обмотки або пластини колектора, обрив секцій якоря та ін.). Такі несправності в електроприводах призводять лише до часткового погіршення працездатності, але активно сприяють подальшому виходу з експлуатації дорогого обладнання.

Тягові електродвигуни відносяться до найбільш навантажених компонентів обладнання з точки зору комплексного впливу на них теплових, електричних, механічних та кліматичних факторів. Тому рівень ушкоджуваності при експлуатації залишається досить високим *(Квасніков В. П., Квашук Д. М., Катаєва М. О., 2021)*.

Статистика відмов силового електромеханічного обладнання показує, що найчастіше двигуни потрапляють у ремонт з причин пробою ізоляції та міжвиткових замикань обмотки якоря – до 25 %; порушення комутації (круговий вогонь) – 12 %; ушкоджень якірних підшипників – 14 – 16 % *(Бондар Б. Є., Очкасов О. Б., Черняєв Д. В., Шевченко І. Я., 2013)*. Розглянуті та більшість інших видів ушкоджень ТЕП супроводжуються змінами температурних режимів експлуатованих механізмів. Перевищення температури супроводжує зниження ресурсу роботи окремих компонентів і тому дуже важливо мати об’єктивну інформацію про нагрівання пристроїв у реальному часі. У зв’язку з цим при діагностичному прогнозуванні неполадок ЕМО важливе місце

займають тепловий аналіз подій із застосуванням математичних моделей цих пристроїв, але в справному стані. Математичні описи дозволяють передбачати можливі інтервали зміни температури частин силового електрообладнання як при навантаженнях, так і за наявності дефектів в них *(Квасніков В. П., Квашук Д. М., Катаєва М. О.,2021).*

Отримання експериментальної інформації потребує наявності локальних засобів вимірювання температури. Достатньо докладну інформацію про температурне поле ТЕП також можна попередньо отримати теоретичним шляхом за допомогою рівнянь теплопровідності. Однак такі математичні моделі забезпечують картину поля, якщо є надійні відомості про розподіл втрат, властивості матеріалів, перебіг процесів охолодження тощо *(Gunal S., Gokhan Ece D., Gerek O.N., 2009)*. Вирішення перелічених завдань за допомогою сукупності обчислювально-програмних засобів у свою чергу потребує оснащення рухомого транспорту відповідною додатковою технікою.

Найбільшої привабливості набувають локальні засоби контролю з дистанційно розміщеними пристроями прогнозування можливих несправностей у транспортному устаткуванні *(Есаулов С. М., Бабичева О. Ф., Шавкун В. М., 2008)*. Подібні пристрої привертають до себе увагу тим, що розміщуються поза РО і можуть застосовуватися для контролю та діагностики дефектів у типових комплектах електромеханічного та мехатронного обладнання, які присутні в сучасному рухомому складі, що серійно випускається *(Есаулов С. М., Бабичева О. Ф., Лукашова Н. П., 2009)*.

Стохастичний характер використання потужності тягових електроприводів на електротранспорті супроводжується змінним нагріванням компонентів ЕМО, що пов’язано з частотою реалізації динамічних режимів пуску, гальмування, інтенсивності пасажиропотоку, впливом навколишнього середовища та інших факторів *(Єсаулов С. М., Бабічева О. Ф., Акіньшин Д. О., 2021)*.

Змінні умови експлуатації електротранспорту сприяють прояву дефектів також у струмопередаючих елементах, колекторних щітках, відсутність мастила, механічному зносі, забрудненні підшипників та ін.

Зазначені причини відображають доцільність вивчення теплових процесів в ЕМО для виявлення причин надлишкового тепловиділення та вибору шляхів їх аналізу з можливістю керування тепловими процесами під час експлуатації обладнання.

Таким чином синтез ефективних технічних засобів для контролю, діагностики та управління процесом нагрівання частин силового електромеханічного обладнання є **завданням важливим**, рішення якого сприяє підвищенню надійності при довготривалій експлуатації технічних рішень в умовах впливу багатьох небажаних факторів.

1. Дослідження пристрою контролю теплових умов при експлуатації електромеханічного обладнання.

Моделювання та контроль теплових процесів у силовому електрообладнанні. Нагрів електричних двигунів при своїй роботі визначається допустимою температурою, яка визначається нагрівостійкістю застосовуваних ізоляційних матеріалів його обмоток. Враховуючи обмеження за допустимою температурою нагріву, що гарантують нормативні терміни служби обладнання, очевидно, що нагрівання електродвигуна відноситься до важливих параметрів контролю протягом усього терміну експлуатації будь-якої електричної машини. На підставі існуючих вимог сутність перевірки двигуна нагрівання зазвичай полягає в зіставленні допустимої температури нагріву з величиною, яку пристрій має при роботі *(Есаулов С. М., Бабичева О. Ф., Шавкун В. М., 2008)*. При оцінці нагріву важлива не абсолютна температура електроприводу, а перегрів *T*, який є різницею температур конкретної частини ЕМО t і навколишнього середовища $t_{ос}$, °С:

$$T = t - t_{ос}, \tag{1}$$

Оскільки при перегріві, наприклад, електродвигуна передбачається контроль допустимого теплового режиму, то цю умову можна записати у вигляді

$$T_{раб} < T_{доп}, \tag{2}$$

де $T_{доп}$ – допустимий перегрів двигуна, який визначається класом його ізоляції, ºС;

$T_{раб}$ – перегрів під час роботи двигуна, ºС.

Практичне використання перевірки двигуна за нагрівом (2) передбачає розрахунок та побудову кривої перегріву $T_{(0)}$ за цикл роботи двигуна *(Єсаулов С. М., Бабічева О. Ф., Ковалик М. М., 2019)*. Точний опис процесів нагріву та охолодження ТЕП є досить складним завданням, яке при аналізі теплових режимів розглядають, приймаючи цілий ряд припущень: однорідність матеріалів електродвигуна, що мають нескінченно більшу теплопровідність та однакову температуру у всіх точках частин корпусу; тепловіддача у зовнішнє середовище пропорційна першому ступеню різниці температур двигуна та навколишнього середовища; навколишнє середовище має нескінченно велику теплоємність, що гарантує незалежність процесу нагріву двигуна від температури; теплоємність двигуна та його тепловіддача, які залежать від температури (для ТЕП $T_{ос}=40$ ºС). В результаті можна записати наступне вихідне рівняння теплового балансу:

$$\Delta P \cdot dt = A \cdot T \cdot dt + C \cdot dt - V \cdot dt, \tag{3}$$

де T – перевищення температури щодо температури навколишнього середовища, ºС;

ΔP – сумарні втрати потужності у ТЕП, Вт;

A – коефіцієнт тепловіддачі електродвигуна у навколишнє середовище за 1с при різниці температур двигуна та навколишнього середовища 1°С, Дж/(°С);

C – теплоємність двигуна для нагрівання на 1°С, Дж/°С;

V – коефіцієнт охолодження електродвигуна з додатковим вентилятором, Дж/(°С).

Розв'язання диференціального рівняння (3) при $\Delta P = const$ має вигляд

$$T = T_{уст} + \left(T_{нач} - T_{уст}\right) \cdot \exp\left(-t / T_{н}\right), \tag{4}$$

де $T_{нач}$ – початкове перевищення температури двигуна над температурою навколишнього середовища $T_{ос}$;

$T_{уст} = \Delta P/A$ – перевищення температури двигуна, що встановилося;

$T_{н} = (C\text{-}V)/A$ – постійна часу нагрівання електродвигуна з вентилятором, с.

Оскільки постійна часу нагрівання $T_{н}$ залежить від часу нагріву ТЕП до встановлюваного перевищення температури $T_{уст}$ за умови відсутності віддачі тепла у навколишнє середовище, то при $T_{нач} = 0$ рівняння (4) набуде вигляду

$$T = T_{уст}\left(1 - \exp\left(-t/T_{н}\right)\right), \tag{5}$$

а при охолодженні з $T_{нач}$ до температури навколишнього середовища, прийнявши величину $T_{уст} = 0$, вираз (5) можна представити

$$T = T_{нач}\left(1 - \exp\left(-t/T_{н}\right)\right). \tag{6}$$

При змінних величинах потужності на валу ТЕП процес тепловіддачі електродвигуна залежить від припливу охолоджувального повітря і ефективності роботи реальної системи вентиляції. Для електродвигунів із самостійною та примусовою вентиляцією доцільно враховувати коефіцієнт погіршення умов охолодження V_{β} силового електроустаткування. Середні значення коефіцієнта V_{β} при пуску, гальмуванні, змінних умовах руху на міських дорогах з урахуванням факторів довкілля часто використовують табличні дані *(Єсаулов С. М., Бабічева О. Ф., Ковалик М. М., 2019)* чи результати спеціальних досліджень. Беручи до уваги величину $T_{уст}$, за номінальних втратах $V_{\beta 0}$ і незмінному значенні теплопровідності матеріалів, перевищення температури ТЕП, що встановилася, запишеться у вигляді

$$T_{уст.н} = \left(\Delta P_{н} / A\right). \tag{7}$$

Якщо втрати електродвигуна дорівнюють або менше номінальних $\Delta P_{н}$, то нагрівання пристрою ніколи не перевищить допустимий рівень. Незважаючи на деяку різницю реально

допустимих від нормованих величин, втрати в ТЕП при змінній температурі нагріву з деякими припущеннями можна розглядати застосовними до об'єкта, що має детерміновані властивості. Таке припущення дозволяє перевірку виконання умови нагрівання компонентів ТЕП представити залежністю

$$T_{\max} \le T_{доп}. \tag{8}$$

Цю умову можна прийняти з метою оцінки справності електрообладнання, експлуатованого у реальному часі. Якщо за допомогою формули (4) отримати залежність $T(t)$ і за нею визначити $T_{\max}$, то залежність (8) може використовуватися при автоматизації діагностичного аналізу справності частин електроприводів з нагрівання їх, застосовуючи автономний обчислювальний пристрій.

Оскільки графік руху електротранспорту на міських маршрутах досить надійно дотримується, цей фактор сприяє застосуванню оцінки середніх втрат струму, моменту або потужності ТЕП за відомий цикл роботи РО, як найбільш зручний для діагностичного аналізу за допомогою будь-якого методу розрахунку обраної еквівалентної електричної величини *(Deuszkiewicz P., Radkowski S., 2003)*. Наприклад, метод середніх втрат може бути використаний як універсальний для аналізу теплових процесів у ТЕП. Визначивши середні втрати потужності $\Delta P_{ср}$, для всього робочого циклу РО або окремих інтервалів його цю величину надалі можна зіставляти з аналогічними розрахунковими номінальними втратами потужності $\Delta P_{н}$. Розглядаючи цикл роботи ТЕП для $T_{ср} = const$, коли кількість теплоти, що аккумулюється в електромашині, приймається дорівнюючою нулю, рівняння теплового балансу (3) можна представити наступною залежністю

$$\int_0^{T_ц} \Delta P \cdot dt = A \cdot T_{ср} \cdot T_ц, \tag{9}$$

звідки отримаємо вираз

$$T_{ср} = \left(1 / A \cdot T_ц\right) \int_0^{T_ц} \Delta P \cdot dt = \Delta P_{ср} / A, \tag{10}$$

де $\Delta P_{ср} = \left(1 / T_ц\right) \int_0^{T_ц} \Delta P \cdot dt$ $\Delta P_{ср} = \left(1 / T_ц\right) \int_0^{T_ц} \Delta P \cdot dt$ – середні втрати потужності за цикл.

Умови (7), (8) та середні втрати теплового режиму експлуатації ТЕП додатково дозволяють отримати більш зручний вираз для теплового діагностичного контролю справності обладнання:

$$\Delta P_{ср} =\le \Delta P_H = P_H \left(1 - \eta_H\right) / \eta_H. \tag{11}$$

де η_H – ККД електродвигуна при номінальному режимі;

P_H – номінальна потужність електродвигуна.

Якщо на окремих інтервалах робочого циклу (РЦ) $T_{ср}$ рівень навантаження прийняти величиною постійної, то середні втрати потужності на тепло визначаться виразом

$$\Delta P_{ср} = \left(\Delta P_1 \cdot t_1 + \Delta P_2 \cdot t_2 + ... + \Delta P_n \cdot t_n\right)/\left(t_1 + t_2 + ... + t_n\right). \quad (12)$$

На підставі (12) очевидно, що розглядуваний метод цілком придатний для вирішення подібних завдань, якщо час роботи двигуна з максимальним навантаженням менше постійного часу його нагрівання T_H, тому що в іншому випадку відбуватиметься значне перевищення допустимої температури нагрівання обладнання. Чим більше значення T_H перевищуватиме величину $T_{\max}$

$$T_H > T_{\max}, \quad (13)$$

тим інтенсивніше скорочуватиметься відстань між параметрами $T_{ср}$ та $T_{\max}$, негативно впливаючи на технічний стан компонентів ТЕП. Найбільш ефективний контроль температури для діагностичного аналізу повинен здійснюватися з точністю щонайменше *±0,5 ºС (Єсаулов С. М., Бабічева О. Ф., Ковалик М. М., 2019).*

Враховуючи відомий взаємозв'язок втрати потужності в двигунах на тепло з квадратом струму в його обмотках, очевидно, що еквівалентну величину струму I_e для різних режимів роботи електродвигуна на всіх інтервалах РЦ можна використовувати і при вирішенні задач діагностичного аналізу розглядуваних параметрів.

Величину еквівалентного струму I_e, що викликає зміни температури обладнання аналогічну реально змінювальному струму на характерних інтервалах РЦ (з підйомами, найбільшим пасажиропотоком тощо), можна представити залежністю

$$I_e = \left(\left(1/T_ц\right) \cdot \int_0^{T_ц} T_ц(t)dt \right)^{0,5} = \left[\left(I_1^2 t_1 + I_2^2 t_2 + ... + I_n^2 t_n\right)/\left(t_1 + t_2 + ... + t_n\right)\right]^{0,5}. \quad (14)$$

У цьому випадку умовою нормованої оцінки нагріву може бути вираз вигляду:

$$I_e \le I_{ном}. \quad (15)$$

Прийнявши незмінними початкові умови постійних втрат потужності на тепло $\Delta P_{ср}$, залежність (15) для методу середніх втрат можна використовувати для обробки даних контролю струму лише на окремих ділянках маршруту або контактної мережі МЕТ, які доступні на

енергопостачальних тягових підстанціях. Ця обставина істотно спрощує вирішення завдання контролю за навантаженням у реальному часі без встановлення автономного спеціального обладнання на рухомому складі.

Для врахування змінних умов охолодження ТЕП на маршрутах руху транспорту у міських умовах вираз (14) з урахуванням величин $V\beta_n$ можна записати у вигляді

$$I_e = \left[\left(I_1^2 t_1 + I_2^2 t_2 + ... + I_n^2 t_n\right)/\left(V\beta_1 \cdot t_1 + V\beta_2 \cdot t_2 + ... + V\beta_n \cdot t_n\right)\right]^{0,5}. \quad (16)$$

Цей вираз (16) переважно застосовувати для однотипних РО зі змінними режимами експлуатації електроприводів, тому що за допомогою параметра $V\beta_n$ можна враховувати комплексний вплив електричних, механічних та кліматичних факторів, включаючи продуктивність засобів примусової вентиляції. Приклад змінних навантажень на фрагменті електронного запису робочого циклу ілюструє рисунок 1.

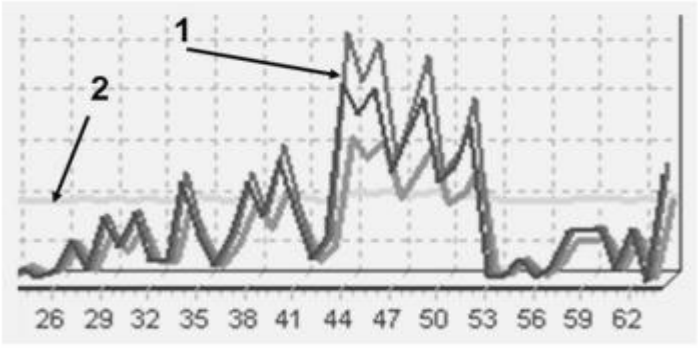


Рисунок 1 – Фрагмент електронного запису навантаження ТЕП на ділянках робочого циклу: 1 – струм навантаження; 2 напруга контактної мережі

Розглянутий вище взаємозв'язок параметрів, що впливають на нагрівання частин ТЕП у реальних умовах, враховувався при моделюванні РЦ, коли були проведені експериментальні дослідження з використанням лабораторного комплекту обладнання. Фізичну модель ТЕП було реалізовано з урахуванням двох електродвигунів постійного струму. Один електродвигун виконував функцію тягового електроприводу (ТЕП), а другий навантаження на валу із завданням змінних реверсивних режимів його експлуатації. При експериментах нагрівання електродвигуна щодо температури довкілля контролювалося за допомогою електронного диференціального термометра. При цьому фіксувалися зазначені режими нагріву конкретних частин ТЕП, що встановилися. Лабораторний термометр включав дві термопари ХК, формувач інформаційного сигналу з напругою U_{MV} від 0,2 до 2 В та низькочастотний генератор (НЧГ) *(Єсаулов С. М., Бабічева О. Ф., Ковалик М. М., 2019)*. НЧГ застосовувався для перетворення вихідної інформації про нагрівання ТЕП за принципом «параметр-частота» (Т-Ч). Частота

вихідного інформаційного сигналу $S_{ТЧ}$ перетворювача Т-Ч від температури T нагрітого вузла визначається залежністю:

$$S_{ТЧ} = f(U_{МУ}, T, C_i), \tag{17}$$

де $U_{МУ}$ – нормований вихідний сигнал вимірювальної схеми з датчиком температури T;

C_i – ємність конденсаторів, що визначають опорну частоту модулятора-перетворювача Т-Ч.

У лабораторному пристрої Т-Ч вихідний сигнал відрізнявся достатньою лінійністю, забезпечуючи при цьому точність вимірювань, з помилкою *±0,4 ºС* та можливістю змінювати чутливість приладу на 1 ºС. Оскільки сигнал $S_{ТЧ}$ можна передавати на відстані без проводів, його вибір був виправданий можливістю застосовувати безконтактний засіб дистанційного контролю нагріву частин ТЕП із застосуванням приймально-передавального комплекту в діапазоні високих частот. Приймально-передавальний комплект включав високочастотний генератор (ВЧГ) з формувачем режиму балансної модуляції на несучій частоті з гармонійним коливанням

$$U_H(t) = U_m \cos\cdot \omega_0 t_н. \tag{18}$$

Формувач сигналу односмугової амплітудної модуляції, містив два фазообертачі (*Ф1, Ф2*). Такий комплект забезпечує зсув фази рівний $\pi/2$ для подальшого перетворення кількох інформаційних сигналів у балансних модуляторах (*БМ1, БМ2*) та суматорі (*SM*).

При вступі на входи першого БМ1 інформаційного сигналу вигляду

$$s(t) = S_0 \cos\Omega t \tag{19}$$

та коливань несучої частоти $U_H(t)$ (18) на виході *БМ1* виходив сигнал згідно з виразом:

$$U_{BM1}(t) = k_{AM} U_m \cos(\omega - \Omega)t + k_{AM} U_m \cos(\omega + \Omega)t. \tag{20}$$

На другому балансному модуляторі *БМ2* при вхідних сигналах, що надходять через інвертори фаз у вигляді

$$U_{ф1}(t) = S_0 \sin \Omega t; \tag{21}$$

$$U_{ф2}(t) = S_0 \sin \omega_0 t, \tag{22}$$

результуючими були коливання, що описуються відповідно до замінних косинусів на синуси, наступним виразом

$$U_{BM2}(t) = 2k_{AM} \cdot U_m \cdot \sin \Omega t \cdot \sin \omega_0 t. \tag{23}$$

З урахуванням відомого тригонометричного співвідношення

$$\sin\alpha \cdot \sin\beta = 0{,}5[\cos(\alpha - \beta) - \cos(\alpha + \beta)], \tag{24}$$

вихідний сигнал *БМ2* можна подати таким виразом

$$U_{BM\,2}(t) = k_{AM} U_m \cos(\omega_0 - \Omega)t - k_{AM} U_0 \cos(\omega + \Omega)t\,. \qquad (.25)$$

При складанні сигналів (19) та (25) у суматорі *SM* отримуємо рівняння вихідного сигналу

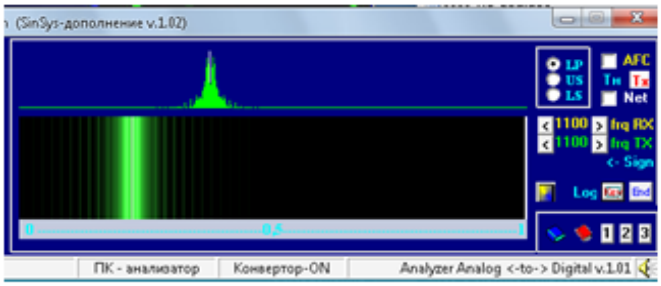
$$U_{SM}(t) = 2k_{AM} U_m \cos(\omega_0 - \Omega)t\,. \qquad (26)$$

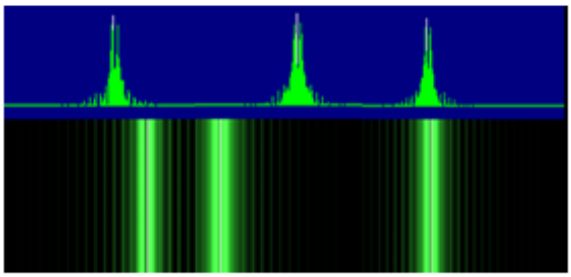
який характеризується однією бічною смугою. Такий сигнал гарантує енергетичний виграш для передавального пристрою *(Єсаулов С. М., Бабічева О. Ф., Ковалик М. М., 2020)*, що використовується з автономним джерелом електроживлення, тому що не випромінює несучий сигнал за відсутності інформаційного повідомлення. Пропонований варіант формування інформаційного сигналу надає можливість одночасно застосовувати кілька локальних НЧГ з різними значеннями опорних частот ω_{o1}, ω_{o2} … ω_{oN}. Для $\omega_{oN} = S_{TЧN}$ можна записати:

$$U_{SM}(t) = 2k_{AM} U_m \cos\left(\left(\sum_{i=1}^{N} S_{TЧN}\right) - \Omega\right)t\,. \qquad (27)$$

де N – кількість тональних інформаційних повідомлень від різних датчиків-перетворювачів «температура – частота».

Зазначені переваги зручні ще й тим, що дозволяють за допомогою кількох датчиків температури одночасно контролювати, нагрівання різних частин ЕМО (корпусів, підшипників, ізоляційних конструкцій, контактів та ін.), передаючи інформацію лише одним бездротовим каналом. Вся сукупність інформаційних повідомлень від передбачених компонентів ЕМО одразу може використовуватися для оцінки градієнта та інших параметрів теплових подій під час експлуатації обладнання. На рисунку 2 представлені експериментальні спектрограми інформаційних повідомлень від одного (а) та кількох (б) перетворювачів Т-Ч з тональною модуляцією. Всі візуальні результати отримані за допомогою лабораторного приймально-передавального пристрою та експериментального аналізатора сигналів у смузі огляду від 200 до 3000 Гц.





«а» *«б»*

Рисунок 2 – Інтерфейси експериментального комп'ютерного аналізатора модульованих сигналів від перетворювачів «температура-частота»: а – контроль монотонного сигналу; б – інформаційні сигнали кількох тональних джерел із частотами $S_{ТЧ1}$, $S_{ТЧ2}$, $S_{ТЧ3}$.

Враховуючи вищевикладені шляхи теоретичних та практичних досліджень для вивчення РЦ ТЕП, було обрано перелік параметрів контролю та запропоновано засоби вимірювання їх із заданою точністю. Комплект експериментальної установки містив регульовані джерела електроживлення, задатчики навантаження на валу та режими примусового охолодження з приладами для вимірювання: I, R – струмів навантаження та гальма, відповідно; U – напруги на клемах електроприводу; V – швидкості потоку охолоджуючого повітря; $S_{ТЧ}$ – частоти інформаційного на виході перетворювача «температура-частота».

Дослідження нагріву обладнання при реалізації робочого циклу. Для моделювання та аналізу експериментальних даних застосовувався класичний факторний аналіз *(Єсаулов С. М., Бабічева О. Ф., Ковалик М. М., 2019)*. Оскільки факторні змінні є лінійною комбінацією вихідних фізичних величин, метод базувався на вибірці показників, що дозволяють сформувати математичний опис об'єкта дослідження з необхідною точністю, зменшуючи при цьому розмірність самої задачі. Враховуючи ефективність застосування ортогональних статечних поліномів при багатофакторному аналізі теплових процесів, для досліджень було прийнято план експериментів з урахуванням змінних режимів експлуатації електродвигунів, що використовуються в дослідній установці. Апроксимацію даних виконували методом найменших квадратів. Перевагою обраного способу є можливість визначення коефіцієнтів метаматематичної моделі ТЕП з реалізацією автоматизації визначення параметрів серед підпрограми матричної алгебри, що входить в різні популярні пакети прикладних програм (Microsoft Office тощо).

План експериментів передбачав реалізацію та варіювання номінальних режимів роботи справного комплекту електрообладнання, представленого в таблиці 1 *(Єсаулов С. М., Бабічева О. Ф., Ковалик М. М., 2019)*.

Таблиця 1 – План реалізації робочого циклу для моделювання номінального режиму нагрівання тягового електроприводу

№ оп.	***I***	***U***	***Ir***	***V***	*№ оп.*	***I***	***U***	***Ir***	***V***
1	**1**	**1**	**1**	**1**	*13*	**1**	**1**	**-1**	**-1**
2	**-1**	**1**	**1**	**1**	*14*	**-1**	**1**	**-1**	**-1**
3	**1**	**-1**	**1**	**1**	*15*	**1**	**-1**	**-1**	**-1**
4	**-1**	**-1**	**1**	**1**	*16*	**-1**	**-1**	**-1**	**-1**

5	**1**	**1**	**-1**	**1**	*17*	**-2**	**0**	**0**	**0**
6	**-1**	**1**	**-1**	**1**	*18*	**2**	**0**	**0**	**0**
7	**1**	**-1**	**-1**	**1**	*19*	**0**	**-2**	**0**	**0**
8	**-1**	**-1**	**-1**	**1**	*20*	**0**	**2**	**0**	**0**
9	**1**	**1**	**1**	**-1**	*21*	**0**	**0**	**-2**	**0**
10	**-1**	**1**	**1**	**-1**	*22*	**0**	**0**	**2**	**0**
11	**1**	**-1**	**1**	**-1**	*23*	**0**	**0**	**0**	**-2**
12	**-1**	**-1**	**1**	**-1**	*24*	**0**	**0**	**0**	**2**

Результати контролю нагріву ТЕП подано на рисунку 3.

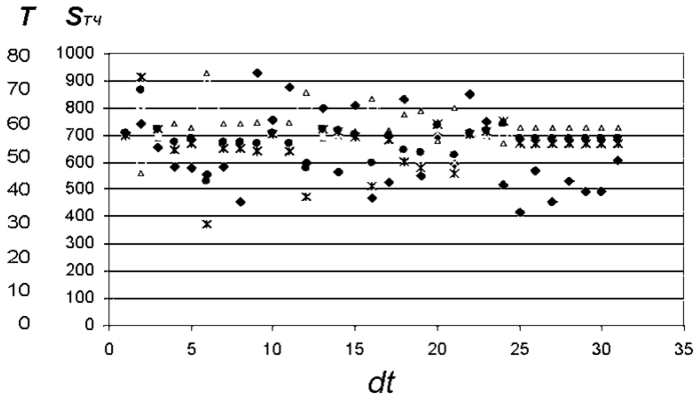


Рисунок 3 – Середні величини параметра нагрівання електроприводу при варіюванні номінальних значень вхідних факторів: T – диференційне значення температури нагрівання, *°C*; $S_{TЧ}$ – частота вихідного сигналу перетворювача «температура-частота», *Гц*; dt – умовні ділянки РЦ

Усі експерименти проводилися за наступних обмежень:

$$\begin{aligned} &-(2+\Delta I) <= I <= +(2+\Delta I);\\ &-(2+\Delta U) <= U <= +(2+\Delta U);\\ &-(2+\Delta R) <= R <= +(2+\Delta R);\\ &-(2+\Delta V) <= V <= +(2+\Delta V). \end{aligned} \quad ; \tag{28}$$

Для моделювання нагріву дослідного ТЕП при реалізації РЦ використовувався регресійний аналіз, відповідно до якого визначалися коефіцієнти апроксимуючого полінома $S_{TЧ}$ вигляду

$$\begin{aligned} S_{TЧp} &= b_0 + b_1 I + b_2 U + b_3 R + b_4 V + ... +\\ &+ b_n N + b_{12} IU + ... + b_{(n-1)n} N_{n-1} N_n +\\ &+ b_{11} I_1^2 + b_{22} U_2^2 + ... + b_{nn} N_n^2 + ... \end{aligned} \tag{29}$$

Прикладний шлях вибору математичного опису враховував вимоги до точності апроксимації, щоб у подальшому за допомогою пристрою технічної діагностики можна було визначати можливі несправності обладнання з оповіщенням цієї події всім передбаченим зовнішнім користувачам, що входять до єдиної мережі для дистанційного контролю та

управління технологічним об'єктом. Оскільки необхідну точність апроксимації можна досягти за рахунок процедури вибору порядку регресійного аналізу, була передбачена можливість використання обчислювальної техніки для практичного застосування математичних описів в умовах реальної експлуатації рухомого транспорту. Виходячи з вищесказаного, задовільну точність вдалося отримати за допомогою регресійної моделі другого порядку. Для даного полінома було виконано розрахунок коефіцієнтів виходячи з результатів вимірів понад 96 груп вхідних величин. Коефіцієнти апроксимуючого полінома мали величини, подані в таблиці 2.

Таблиця 2 – Значення коефіцієнтів апроксимуючого полінома

Коефіцієнти регресії	Розмір коефіцієнта	Коефіцієнти регресії	Розмір коефіцієнта	Коефіцієнти регресії	Розмір коефіцієнта
b_0	419,24	b_{11}	47,19	b_{12}	-26,37
b_1	75,83	b_{22}	33,47	b_{13}	-15,04
b_2	37,54	b_{33}	58,32	b_{14}	-52,54
b_3	64,78	b_{44}	35,87	b_{23}	14,74
b_4	-58,37				

На рисунку 4 ілюструються усереднені дані експериментів $S_{TЧ}$ та розраховані $S_{TЧp}$ методом регресійного аналізу. Враховуючи особливості формування сигналів перетворювача «Т-Ч», всі розрахункові величини округлялися до цілих значень з точністю *±1 Гц*. Розбіжність між $S_{TЧp}$ та $S_{TЧ}$ склало *5,4 %*. Оскільки не можна встановити, чи залежить вид розподілу помилки вимірювань від значень вхідних параметрів, додатково було проведено аналіз залишків між $S_{TЧp}$ та $S_{TЧ}$. Виявилося, що помилки вимірів у всьому інтервалі зміни вихідної величини виявилися досить рівномірно розподіленими. При середньоквадратичному відхиленні, що досягає *14 Гц*, межа помилки контрольованої реальної температури не перевищувала *±2 ºС*, що говорить про задовільний опис робочого циклу та можливість використання його в подальших дослідженнях.

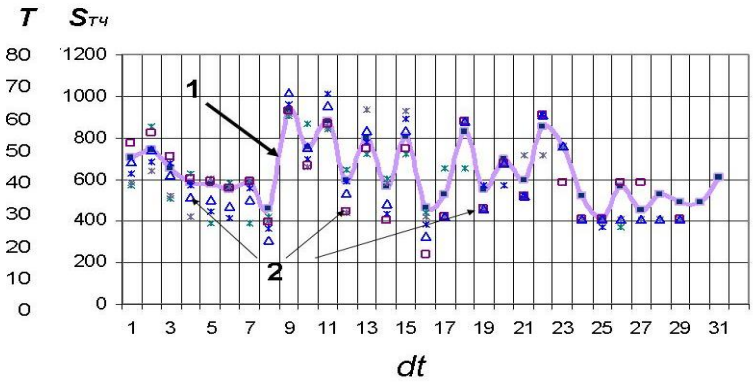


Рисунок 4 – Результати контролю та моделювання нагріву частин корпусу ТЕП при експериментальному робочому циклі: 1 – моделювання; 2 – експеримент

Пристрій контролю та діагностування умов нагріва компонентів електромеханічного обладнання. В отриманому поліномі (29) сила впливу кожного фактора оцінюється коефіцієнтом при ньому, а додаткові компоненти рівняння регресії дозволяють виділяти перехідні області механізму процесу нагрівання всіх частин ТЕП та інтерпретувати теплові події, що важливо при ідентифікації можливих поломок, користуючись таким виразом. Сімейства імпульсних кривих (рис. 5), що відображають параметричну чутливість теплових процесів до всіх обраних вхідних величин, допомагають ідентифікувати градієнти температури з можливими конкретними несправностями частин обладнання *(Єсаулов С. М., Бабічева О. Ф., Ковалик М. М., 2020)*.

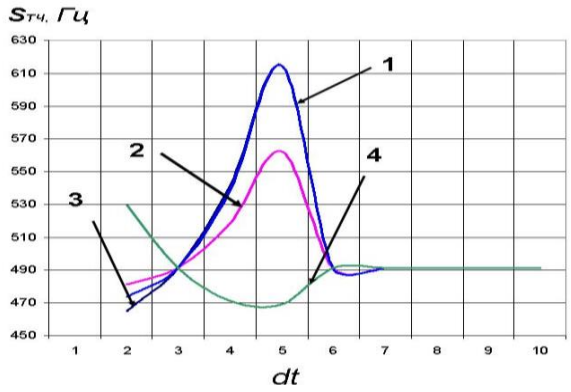


Рисунок 5 – Аналіз параметричної чутливості теплових процесів при імпульсному варіюванні вхідних величин: 1 – струм; 2 – напруга; 3 – навантаження; 4 – охолодження

Скориставшись виразами (4) та (27) за допомогою (29) додатково було отримано допустиму варіативну зону (рис. 6) для діагностичного контролю нормованого нагрівання частин ТЕП на всіх експериментальних інтервалах РЦ.

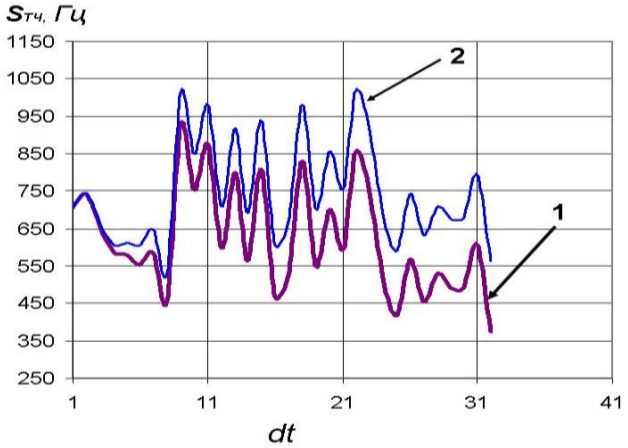


Рисунок 6 – Варіативна зона нормованого нагрівання ТЕП:

1 – нижній рівень; 2 – верхній рівень

З рисунку 6 видно, що діагностичний контроль нагрівання частин ТЕП переважно розташований поза верхнього рівня варіативної зони. Такі величини можна розцінювати як можливі неполадки. Доповнивши систему контролю додатковими датчиками для вимірювання градієнта температури в зонах «корпус-підшипник», «корпус-клеми», «корпус-ізоляція» тощо, можна підвищити селективні властивості вимірювального пристрою та підвищити точність ідентифікації неполадок у різних частинах силового електроустаткування.

Застосування отриманих результатів в експериментальному комплекті приладу для діагностичного контролю справності ТЕП за допомогою спектрографа ілюструють рисунки 1.7, 1.8 *(Єсаулов С. М., Бабічева О. Ф., Ковалик М. М., 2020)*.

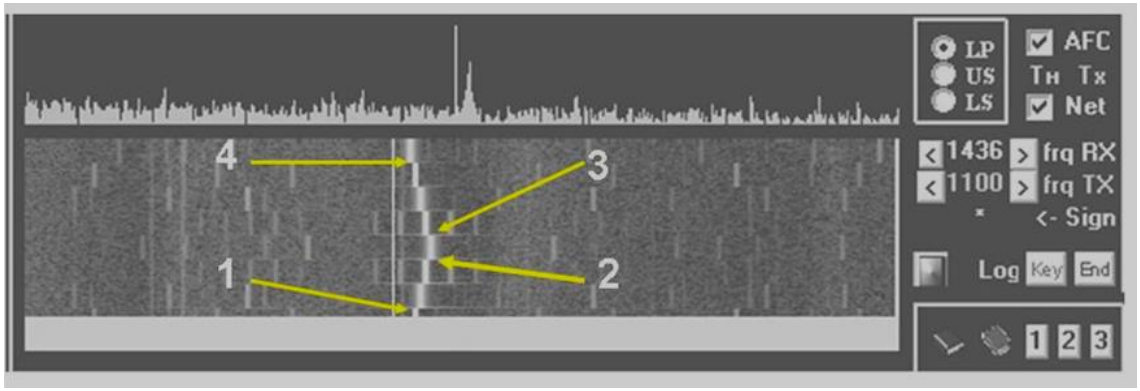


Рисунок 7 – Спектрограма контролю за зміною температури компонента ТЕП: 1 – 2 – нагрівання; 2 – 3 – режим, що встановився; 3 – 4 – охолодження

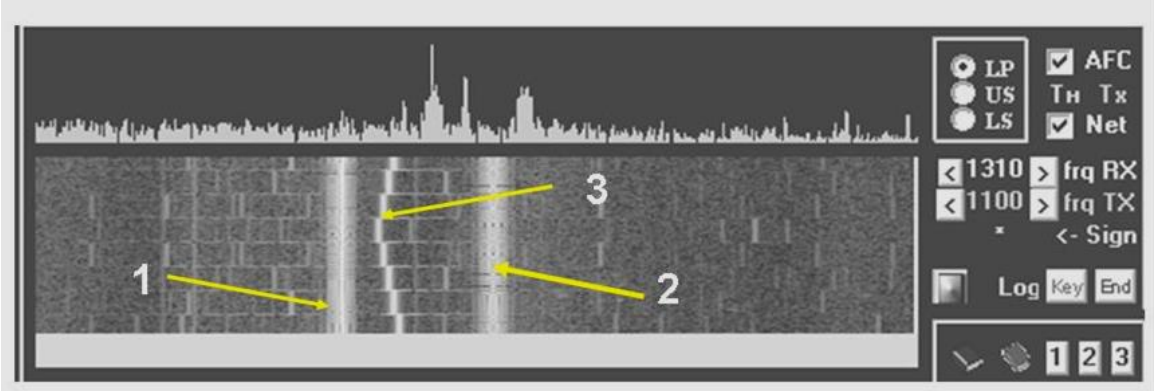


Рисунок 8 – Спектрограма контролю температури з електронними мітками допустимого інтервалу варіювання параметра: 1, 2 – мітки нижнього та верхнього рівнів; 3 – траєкторія дискретної зміни контрольованого параметра

Можливості візуалізації використання розглянутого комплекту вимірювального приладу за умов впливу різних перешкод ілюструє рисунок 9. Даний фрагмент спектрограми отримано при рівні інформаційного сигналу *–13,7dB* і відповідає умовам, коли перешкоди в 5,3 рази переважали над корисним сигналом від датчика *(Єсаулов С. М., Бабічева О. Ф., Рогожина Х. О., 2019)*.

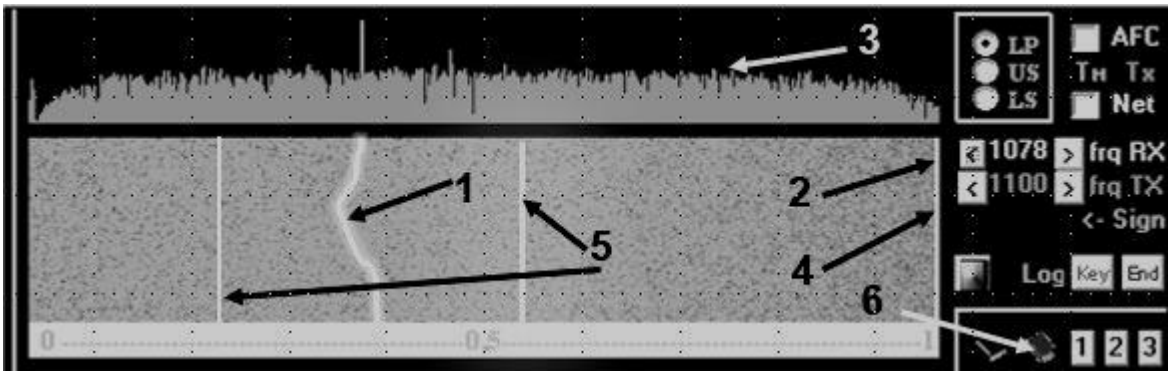


Рисунок 9 – Спектрограма контролю температури за умов перешкод:
1 – траєкторія контрольованого параметра; 2 – табло частоти контрольованого параметра, Гц; 3 – рівень перешкод у смузі контролю інформаційних повідомлень від термодатчика-перетворювача; 4 – табло несучої частоти конкретного термодатчика, Гц; 5 – рівні допустимого варіювання сигналу конкретного термодатчика; 6 – виклик журналу запису інформаційних повідомлень від термодатчика-перетворювача.

Аналіз експериментальних спектрограм показав, що у мітках меж варіативної зони (рис. 8) може відбуватися зниження точності вимірів. Ця обставина негативно впливає на результати роботи вимірювального пристрою. Очевидний шлях вирішення цієї проблеми можливий шляхом регулювання потужності джерел сигналів, а також вибору чутливості вбудованого частотоміра. Варіанти підвищення порядку полінома, що використовується в програмній частині частотоміра, може призвести до зайвої громіздкості математичного виразу (29), що не може гарантувати підвищення якості аналізу аналізатора інформаційних повідомлень. Крім того, зазначений недолік можна також усунути, підвищивши рівень апроксимації моделі лише на характерних інтервалах робочого циклу з урахуванням залежностей

$$\begin{array}{l}(2+\Delta I)\le I\le I_m;\\(2+\Delta U)\le U\le U_m;\\(2+\Delta R)\le R\le R_m;\\(2+\Delta V)\le V\le V_m,\end{array}; \qquad (30)$$

де I_m, U_m, R_m, V_m – гранично-допустимі значення технологічних величин.

Останній варіант аналізу контрольованої температури можна використовувати для ідентифікації теплових подій, тому що ретельний вибір масштабу нормованого сигналу U_{MY} допомагає підвищувати діагностичні властивості приладу в оцінці можливих несправностей у локальних технологічних місцях під час контролю температури. На експериментальному стенді налаштування U_{MY} дозволяло варіювати чутливість перетворювача Т-Ч від 3 до 17 Гц при зміні температури $\pm 1^{o}C$. Використання такої можливості забезпечує вибір найбільш прийнятної

чутливості приладу в умовах перешкод, особливо найбільш відповідального верхнього граничного рівня допустимої зони варіювання контрольованої ординати (рис. 8). В експериментальному варіанті приладу гранична чутливість (*±1Гц*) при змінах температури змінювалася в інтервалі *±0,15...0,02 ºС*. З підвищенням чутливості виникала потреба вирішення проблеми боротьби із шумами різного походження. Однак, отримані результати дозволяють зробити висновок, що розглянутий комплект приладу підтвердив можливість використання з математичними та візуальними засобами апроксимації для виявлення можливих неполадок у компонентах ЕМО *(Szymański, Z., 2009)*. За допомогою пропонованого засобу контролю можна створювати локальні діагностичні прилади для оцінки справності частин рухомого транспорту, що характеризуються надлишковим тепловиділенням при експлуатації.

2. Автоматизація процесу нагріва електромеханічного обладнання.

Аналіз існуючих систем теплової стабілізації діючого обладнання. На об'єктах комунального господарства технологічні процеси реалізуються спільно зі спеціальними керуючими пристроями, що забезпечують стабілізацію вихідних ординат, до яких належать температури нагрівання та охолодження компонентів електромеханічного обладнання.

Розглянуті раніше прийоми синтезу засобів контролю температури нагрівання обладнання можуть виявитися прийнятними при розробці пристроїв стабілізації нагрівання обладнання, що сприяють довготривалій надійній експлуатації їх.

Основні цілі керування будь-якими об'єктами реалізуються через показники чи керовані параметри за певним законом *(Yesil E.; Guzelkaya M.; Eksin I., 2004)*. У практиці побудови систем автоматичного регулювання (САР) тепловими процесами широко використовуються позиційні та пропорційно-інтегрально-диференціальні (ПІД) контролери або регулятори. При змінах завдань та графіків їх активації, змінному характері навантаження та інших факторах перевагу віддають ПІД-контролерам. На жаль, при постійних налаштуваннях контролера стохастичні процеси призводять до зниження ефективності роботи систем примусового охолодження, що супроводжуються зростанням енерговитрат, щоб уникнути таких небажаних подій доводиться застосовувати ручний спосіб коригування налаштувань системи керування, що знижує переваги автоматики при керуванні процесами та установками з генерацією надлишкового тепла.

Типове завдання налаштування більшості САР може бути сформульована, виходячи із знайденої аналітичної або в результаті обробки даних експериментів передавальної функції об'єкта регулювання. Ще на стадії проєктування передавальні функції допомагають вибирати комплект засобів автоматики, що реалізує необхідний закон регулятора (П, ПІ, ПІД тощо) *(Єсаулов С. М., Хворост М. В. , Бабічева О. Ф. , Найдьонов М. О., 2023)*. У кожному випадку визначення параметрів налаштування керувального пристрою залежить від динамічних

властивостей об’єкта керування і завжди відрізняється оригінальністю, що дозволяє досягти необхідну стійкість і задану якість роботи САР.

Стійкість, тобто згасання процесу регулювання є необхідною, але далеко не достатньою вимогою, яка пред’являється системам автоматичного регулювання. До додаткових вимог відносяться також мінімальна тривалість перехідного процесу, інтенсивність загасання вихідного параметра, обмежене значення граничного відхилення контрольованої ординати від задавального впливу тощо. Щоб керувати складною технічною системою доцільно враховувати найбільшу сукупність факторів, що впливають на технологічний процес, та вміти точно вимірювати вибрані технологічні величини. При кількох взаємопов’язаних контрольованих величин використовують функціональні залежності змінних, включаючи структурні, технічні, апаратні та експлуатаційні характеристики, що практично реалізувати часто викликає значні складності. Зазначені причини вказують на те, що для кожного стану об’єкта управління (ОУ) необхідно правильно підбирати закон регулювання, значення настроювальних коефіцієнтів регулятора, що має бути в повній згоді з подіями на об’єкті. У реаліях використовується лише один набір коефіцієнтів для всіх режимів, а це нерідко перетворює ПІД-контролер на штучний генератор додаткових збурень усередині самої системи керування технологічним процесом.

Для виключення зазначеної проблеми в системі керування важливо передбачити усунення мимовільних збурень, що досягається застосуванням інтелектуальних пристроїв. У тому числі можна назвати реалізацію інженерних прийомів за допомогою нечіткої логіки *(Єсаулов С. М., Хворост М. В. , Бабічева О. Ф. , Найдьонов М. О., 2023)*. Для цього розглядаються безмодельні методи налаштування ПІД-контролера або експертні системи аналогічного призначення. У базах правил таких рішень вказується на скільки відсотків слід змінити амплітудне значення того чи іншого коефіцієнта регулятора залежно від ситуації, що склалася в об’єкті. Оскільки початкову ступінь нелінійності ОУ важко оцінити, то вихідні правила нечіткої системи вносять зміни, що виявляються в процесі роботи обладнання *(Єсаулов С. М., Бабічева О. Ф., Рогожина Х. О., 2019)*. Привабливість цього підходу обумовлена можливістю застосовувати засоби налаштування у вигляді додаткового блоку, що вбудовується в існуючу САР. Внаслідок цього забезпечується незначний захід вартості впровадження подібної інженерної пропозиції у вже діюче обладнання та бажаний результат модернізації засобу автоматики *(Sabri, Laith & Al-mshat, Hussein., 2015)*.

Сучасні САР, що містять у своїй структурі мікроконтролери, стежачі системи, автопілоти, обчислювальні компоненти, пристрої дистанційного керування тощо, часто мають певний набір елементів придатних для їх подальшого вдосконалення. Ця обставина дозволяє формувати резерви електронних ресурсів, які задіяні у подальшому на вирішення можливих інженерних завдань автоматизації технологічних об’єктів. Зі зростанням обчислювальної потужності

компактної мікропроцесорної техніки розширилися можливості застосування програмних рішень реалізації всіх таких інженерних завдань.

Оскільки для стохастичних теплових процесів з автоматикою, що реалізує пропорційно-інтегрально-диференціальний закон управління, важливо мати можливість своєчасно змінювати налаштування регулятора, то дана тема залишається актуальною стосовно систем управління тепловими режимами в об'єктах зі змінними динамічними властивостями.

Аналітичні дослідження теплових процесів. При експлуатації електромеханічного обладнання з електричними приводами останні в тепловому відношенні є складним об'єктом, що містить розосереджені джерела генерації теплоти. Нагрів окремих компонентів залежить від режиму експлуатації, напряму теплових потоків усередині обладнання та в навколишнє середовище, які завжди мають змінний характер. При цьому фактори, що змінюються, залежать від температури навколишнього середовища та умов експлуатації обладнання. Для спрощення аналізу теплових процесів в ЕМО приймають припущення, серед яких можна виділити однорідність та велику теплопровідність генераторів тепла (електродвигунів), навантаження виконавчої частини приводу, втрати потужності, температуру навколишнього середовища, які розглядають незмінними величинами. Теплотою випромінюванням, що віддається, нехтують через невелику кількість цього параметра. Такий підхід *(Єсаулов С. М., Хворост М. В. , Бабічева О. Ф. , Найдьонов М. О., 2023)* дозволяє використовувати закон збереження енергії для складання рівняння теплового балансу

$$\Delta P dt = \Delta A \tau dt + c d\tau , \tag{31}$$

де P – втрати потужності в електроприводі;

A – тепловіддача двигуна у навколишнє середовище;

c – теплоємність двигуна;

τ – перевищення температури двигуна над температурою довкілля;

t – час.

Перетворення виразу (31) дозволяє отримати постійну тривалість нагрівання

$$Tн = c / A , \tag{32}$$

перевищення температури, що встановилося

$$\tau y = \Delta P / A \tag{33}$$

або

$$\tau y = \left(-\frac{\tau}{t} \right) + \tau \tag{34}$$

і остаточний вираз запишеться у такому вигляді

$$\tau = \tau y\left[1-\exp\left(\frac{t}{Tн}\right)\right]+\tau_0\cdot\exp\left(\frac{t}{Tн}\right). \quad (35)$$

Вираз (35) придатний для аналітичного дослідження перехідних характеристик нагрівання двигуна. Отримані таким шляхом експонентні залежності вказують, що процеси нагрівання та охолодження двигуна можуть бути розраховані з урахуванням відомих параметрів двигуна. Рекомендований приблизний облік різних компонентів, що входять до складу ЕМО, на жаль, завжди матимуть змінний характер. Цей факт обумовлений тим, що при постійних масі, ККД та потужності двигуна складно врахувати зовнішні величини, що впливають на самовентилювання та умови примусового охолодження частин електричного приводу. При незмінному закритому виконанні, класі ізоляції та навантаженні на валу характеристики тепловіддачі однотипних електродвигунів (ЕД) завжди відрізнятимуться між собою (рис. 10).

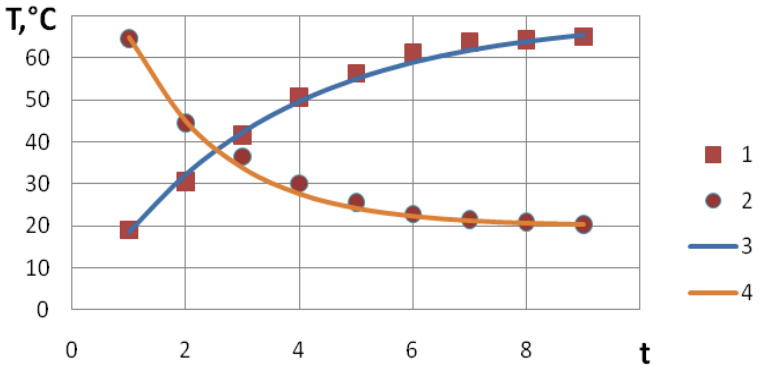


Рисунок 10 – Характеристики нагрівання (1) та охолодження (2) двигуна:
1,2 – експериментальні; 3,4 – аналітичні; T – температура; t – час

Застосування аналітичних прийомів для опису процесів нагріву (криві 1, 3) та охолодження (криві 2, 4) підтверджують монотонність аналізованих процесів з протилежною спрямованістю, що відображають також хаотичний характер динамічних властивостей процесу теплообміну в ЕМО (рис. 11).

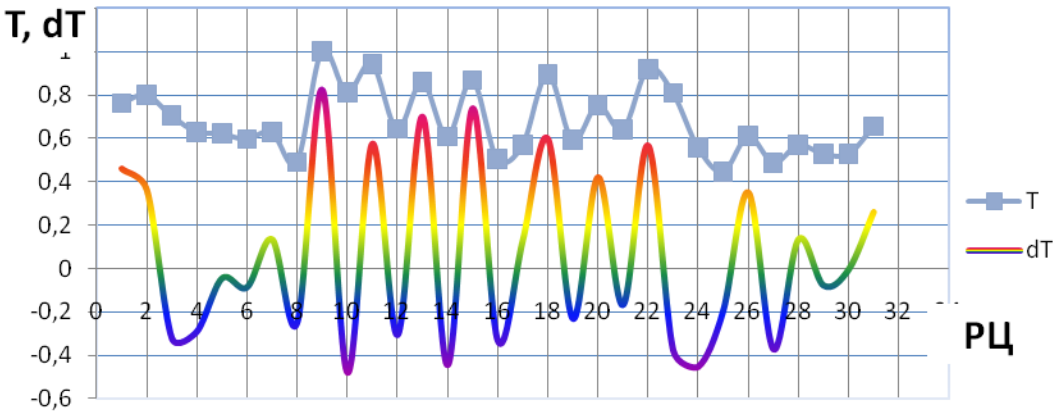


Рисунок 11 – Варіювання нагріву та градієнта температури ЕД при змінних навантаженнях: T – температура; dT – градієнт нагрівання; РЦ – робочий цикл

Різноманітність РЦ силового обладнання з динамічними параметрами, що змінюються, повинна враховуватися в системах автоматики вибором уставок настроювальних параметрів. Оскільки класичні системи стабілізації технологічних величин орієнтовані на хід основного технологічного процесу, то процеси теплообміну контролюють лише з метою виключення критичних подій нагріву обладнання, здатних вивести з ладу дорогі його частини. Разом з цим не виключені ТО, в яких інтелектуальний облік теплових процесів сприяє суттєвому підвищенню економічних показників за рахунок скорочення енерговитрат на тепловиділення.

Синтез пристрою теплоавтоматики на базі ПІД-регулятора. Для побудови інтелектуальної системи управління технологічним процесом відомо багато методів *(Astrom K. J., 2006)*. При вирішенні таких завдань дослідники виділяють пристрої, що реалізують нечіткі алгоритми управління (НАУ) технологічними процесами. Оскільки НАУ мають нелінійні властивості, то завдяки цьому з'являється можливість здійснювати зміну керувальної ординати, змінюючи настроювальні параметри керуючого контролера. Для схеми управління з ПІД-регулятором *(Єсаулов С. М., Хворост М. В. , Бабічева О. Ф. , Найдьонов М. О., 2023)* таке рішення може мати такий вигляд (рис. 12).

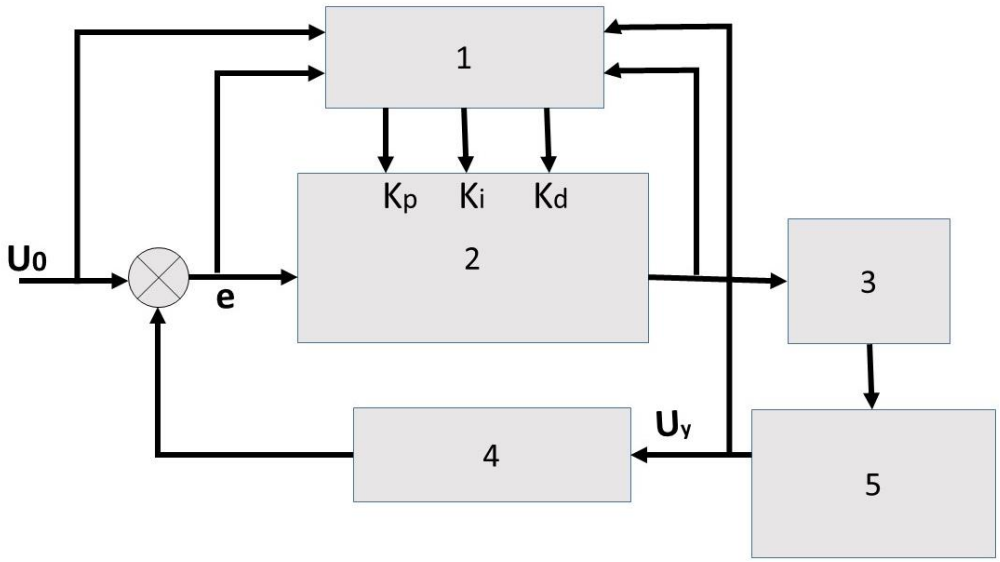
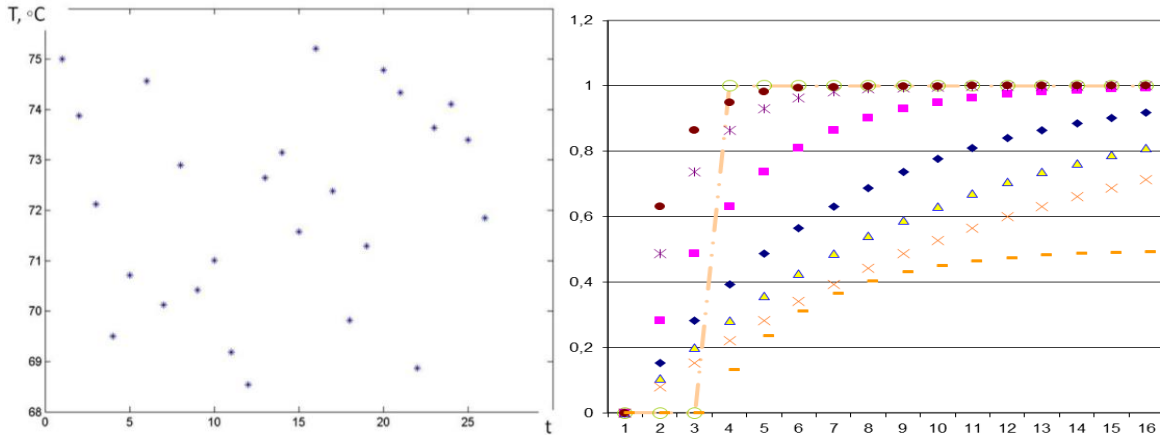


Рисунок 12 – Схема управління з блоком НАУ для коригування параметрів налаштуванням *Kp, Ki, Kd* ПІД-контролера: 1 – блок НАУ, 2 – ПІД-контролер; 3 – виконавчий механізм; 4 – датчик контролю вихідний ординати; 5 – об'єкт управління; U_0 – сигнал завдання; e – неузгодженість; *Uy* – вихідна величина

Для досягнення заданих результатів роботи в такому пристрої необхідно враховувати специфічні властивості ОУ, які передбачаються наборами технологічних подій, що розглядаються

при розробці НАУ. На жаль, на ОУ зі стохастичними властивостями здійснити бажаний набір ситуацій є досить складним.

При аналізі РЦ (рис. 11) виявлено, що в управлінні об'єктом з тепловиділенням необхідно враховувати два різних за своєю природою процесу. До першого слід віднести нагрівання, коли нові значення параметра контролю більші за попередні, а до другого – охолодження, коли контрольована величина зменшується. На ЕМО з примусовим охолодженням обидва ці процеси відбуваються зі змінними швидкостями і тому задані якісні показники перехідних характеристик при постійних налаштуваннях регулятора отримати неможливо (рис. 13).



а б

Рисунок 13 – Варіювання температури (а) та перехідних характеристик нагріву (б) при змінних навантаженнях експлуатації ЕМО

У зв'язку з цим доцільно реалізовувати блок НАУ для коригування керованої величини *Uy* шляхом зміни налаштувань регулятора *Kp, Ki, Kd* у вигляді двох самостійних наборів, кожен з яких авономно відповідає за управління процесами як при нагріванні, так і при охолодженні частин обладнання.

Як експериментальну установку було використано комплект тягового та навантажувального електродвигуна з системою контролю температури нагрівання частин електроприводу. Система управління мала ПІД-контролер з можливістю електронного коригування настроювальних параметрів (рис. 14).

Рисунок 14– Компоненти дослідного комплекту обладнання:

1 – цифровий ПІД-контролер; 2 – експериментальний блок керування

Досвідченим шляхом було визначено транспортне запізнення інформаційного сигналу від різних датчиків температури, яке змінювалося в інтервалі від 8 до 77 с (на корпусі електроприводу, підшипниках, суміжних компонентах тощо).

Дослідження РЦ ЕМО з характерними тенденціями зростання та зниження температури (рис. 2.2) дозволяють зробити висновок, що варіювання тепла завжди супроводжується стохастичними перехідними процесами (рис. 13), що залежать від багатьох неконтрольованих зовнішніх факторів. За допомогою експериментальних даних були отримані передавальні функції *W(p)* можливих каналів керування для різних компонентів обладнання у вигляді

$$W(p) = k \cdot \exp\frac{(-\tau p)}{Tp+1}, \tag{36}$$

$$W(p) = k \cdot \exp\frac{-\tau p}{(T1p+1)(T2p+1)}, \tag{37}$$

де k – коефіцієнт посилення;

T – постійна часу;

τ – транспортне запізнення;

p – оператор Лапласа.

На основі отриманих перехідних характеристик (рис. 13б) було визначено варіації параметрів *Ti* (2,36 – 16,83), *k* (0,42 – 0,97), *τ* (8 – 77 с), які завжди мали змінний характер. Подані факти вказують, що в ідеальному випадку доцільно застосовувати роздільні засоби управління процесами нагрівання та охолодження, що в існуючих системах рідко передбачається.

Параметром контролю ефективності системи автоматики було обрано точність, яка визначається як мінімум середньоквадратичного відхилення вихідної величини *Uy (Єсаулов С. М.,*

Хворост М. В. , Бабічева О. Ф. , Найдьонов М. О., 2023) Для дослідження системи управління з блоком НАУ було використано моделювання ЕМО за допомогою пакету Matlab. У середовищі Simulink використовувалася структура ПІД-регулятора (рис. 15), описана в роботі *(MATLAB, 2000).*

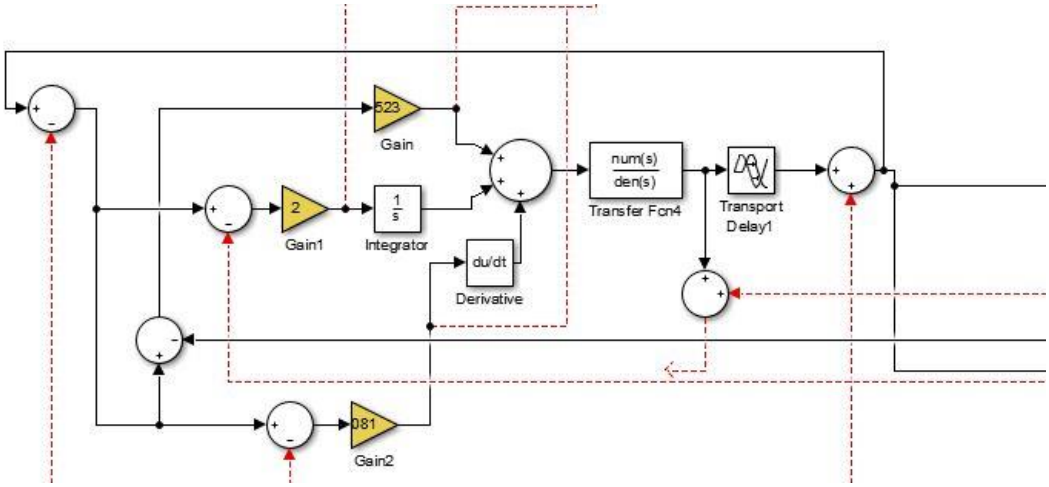


Рисунок 15 – Фрагмент моделі об’єкта ЕМО з ПІД-регулятором

З використанням середовища Fuzzy Logic Toolbox створювалася додаткова структура ПІД-регулятора, що включає блок НАУ (рис. 16).

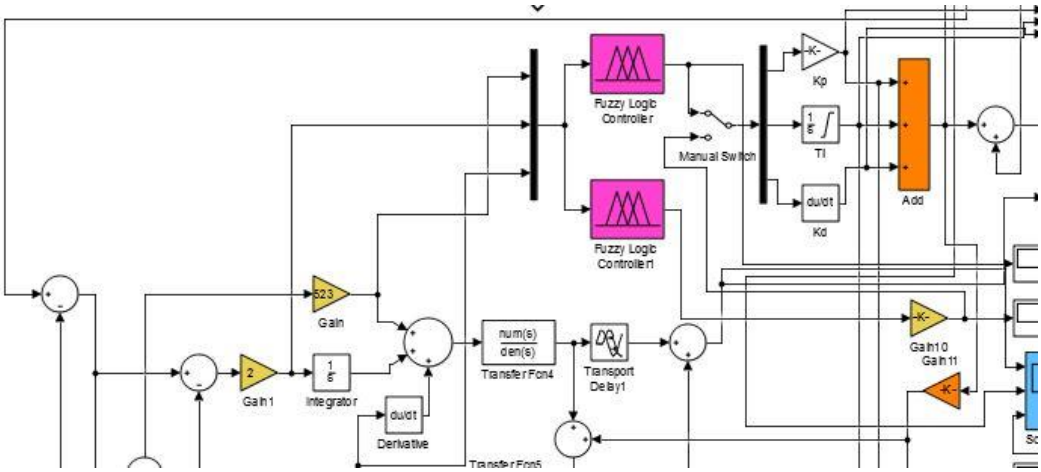


Рисунок 16 – Фрагмент моделі ПІД&НАУ-регулятора

З рисунків 15, 16 можна зробити висновок, що при регулюванні теплових процесів в ЕМО з урахуванням неузгодженості (помилки регулювання) – різниці вхідного сигналу (уставки) і сигналу зворотнього зв’язку формується керуючий сигнал для виконавчого органу. Керуючий сигнал ПІД-регулятора (рис. 15) є сумою пропорційного, інтегрального та диференціального доданків. Вклад кожного доданку в підсумковий керуючий сигнал задається коефіцієнтами. Коефіцієнт *Kp* – пропорційний доданок визначає внесок сигналу неузгодженості в керуючий сигнал, *Ki* – інтегральний доданок визначає внесок інтеграла від сигналу неузгодження за весь час роботи системи управління, *Kd* – диференціальнийдоданок визначає внесок похідної сигналу

неузгодженості. Модель ПІД-регулятора допускає відсутність окремих доданків у керуючій величині, що дозволяє змінювати та порівнювати ефективність законів регулювання при експериментах з ОУ, що відрізняються змінними динамічними параметрами.

Для забезпечення заданих властивостей системи автоматичного управління (швидкості реакції, величини перерегулювання, стабільності параметра) проводилася попередня оцінка діапазону значень коефіцієнтів керуючого контролера за допомогою математичної моделі та виконання ручного додаткового налаштування уставок коефіцієнтів, що на практиці завжди виконується в процесі пуско-налагоджувальних робіт.

Функціонування блоку нечіткого алгоритму управління (рис. 16) було засновано на використанні знань експериментів. Оскільки безліч ситуацій при управлінні об'єктом непостійні через нестабільність та непередбачуваність властивостей об'єкта, використання аналітичних моделей у такому випадку просто недоцільне і тому перевага надається структурним моделям реальної системи, для якої створювався макет блоку НАУ. Блок фазифікації в НАУ перетворює чіткі величини, виміряні на виході технологічного об'єкта, на нечіткі змінні, які описуються лінгвістичними даними в основі знань. Весь алгоритм нечіткого набору передбачав використання популярного алгоритму Сугено *(Єсаулов С. М., Хворост М. В. , Бабічева О. Ф. , Найдьонов М. О., 2023).*

Структурна схема блоку фазифікації серед Simulink була отримана за допомогою інструментарію *Fuzzy Logic Toolbox (MATLAB, 2000)*. У редакторі системи (Fuzzy Inference System Editor) використано тип системи Мамдані із завданням вхідних параметрів: *ε(k)* – значення помилки, *deltaε(k)* – швидкість зміни помилки (похідна), *integralε(k)* – інтеграл помилки. Виходи моделі – коефіцієнти регулятора формувалися за допомогою пристрою на рисунку 17.

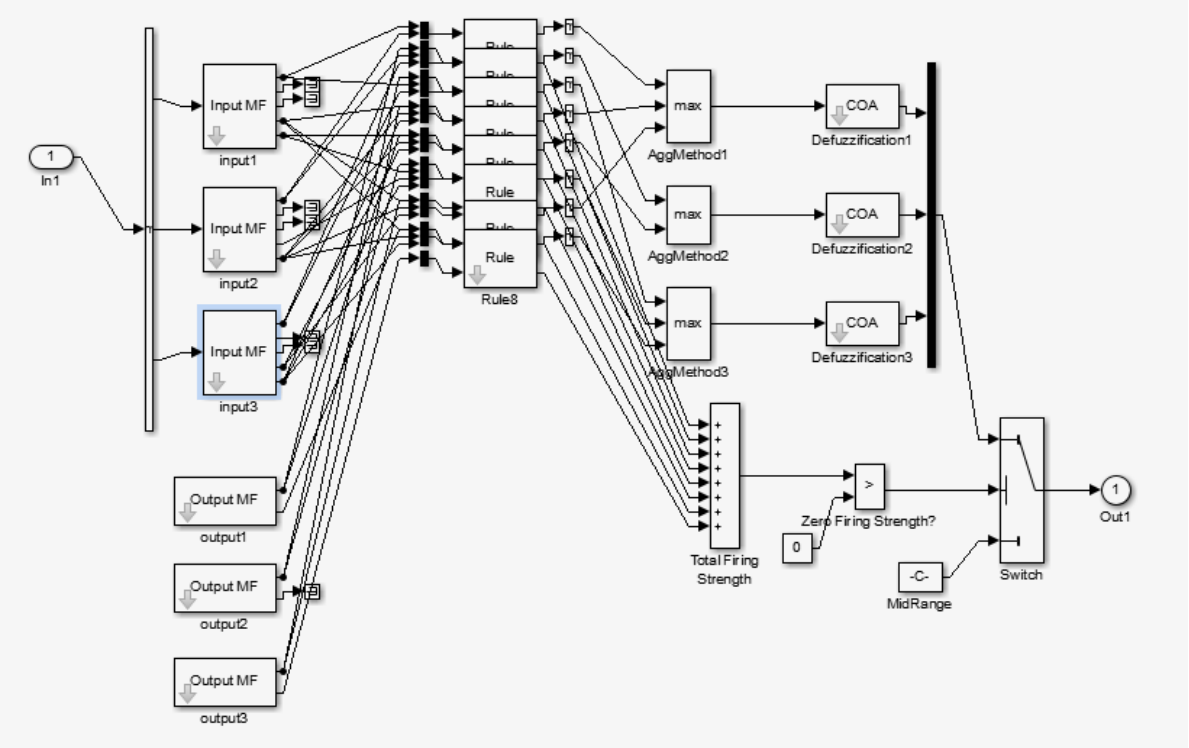
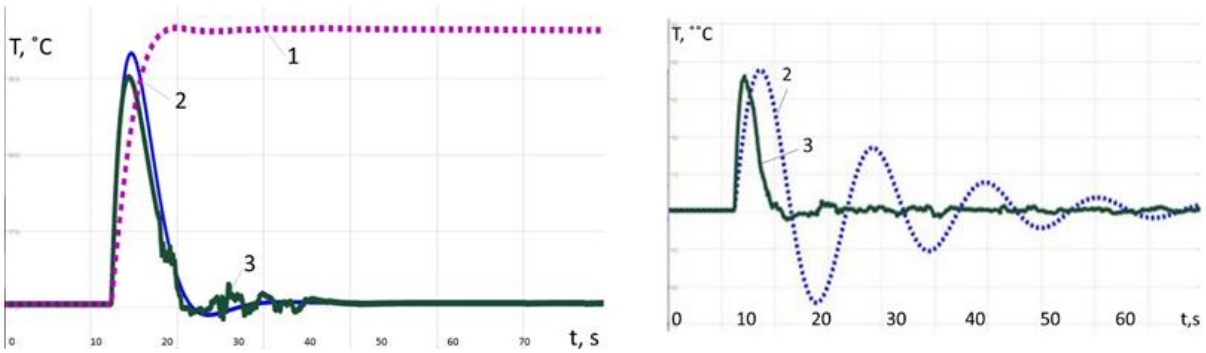


Рисунок 17 – Структура блоку фазифікації у середовищі Simulink за допомогою інструментарію Fuzzy Logic Toolbox

Для незмінної моделі об’єкта (рис. 17) представлені результати роботи експериментальних систем управління, що ілюструють ефективність роботи класичного ПІД-регулятора та застосування його разом із блоком НАУ.

З рисунка 18а видно, що передбачене нагрівання обладнання (72 – 95˚С) з ретельним налаштуванням класичного ПІД-регулятора в системі управління дозволяє протягом *~20 с* вийти на режим із заданим значенням вихідного параметра (крива 2). Помилка регулювання не перевищувала 0,35 %. Аналогічний тепловий режим обладнання з системою управління ПІД&НАУ (крива 1) супроводжується уповільненою реакцією регулювання зі змінною помилкою регулювання 0,32 – 0,76 % протягом ~30 с.



«а» «б»

Рисунок 18 – Результати моделювання систем автоматики:

а – нормований перехідний процес 72 – 95 ºС; б – випадковий перехідний процес 92 – 110 ºС; 1 – перехідний процес нагрівання ЕМО; 2 – система примусового охолодження з ПІД-регулятором; 3 – система примусового охолодження із блоком фазифікації

З рисунка 18б можна зробити висновок, що налаштування ПІД-регулятора при збуреннях (92 – 110 ˚С) неузгоджуються з динамічним властивостями технологічного процесу і характеризуються істотним перерегулюванням (крива 2) тривалий час. Коливання вихідної ординати можна усунути лише переналаштуванням уставок, але це завдання складно виповняти на діючому обладнанні, коли подія сталася. У свою чергу комплект ПІД&НАУ для таких самих аномальних подій в ОУ недовго виконує пошук рішення, що узгоджується із заданим значенням вихідної ординати (крива 3). У цьому відбувається поступовий вихід на заданий режим, супроводжуваний незначними відхиленнями вихідної величини (менше 0,27 %) без істотного перерегулювання. Оскільки пошук настроювальних параметрів у часі був виконаний автоматично, а незначні зміни вихідної величини не перевищували припустимої помилки, розглянутий варіант ПІД-регулятора з блоком фазифікації відрізняється помітними перевагами від класичного ПІД-контролера.

Експериментально було встановлено, що при розширенні інтервалу нагріву до 120˚С система автоматики з ПІД-контролером завжди потребувала переналаштовування, тому що коливальний процес вихідної ординати у часі тривав тривалий час (кілька хвилин). Робота системи автоматики з ПІД&НАУ відбувалася з достатньою стійкістю та варіюванням вихідної ординати

0,2 – 1,3%, що узгоджувалося із завданням припустимої помилки для аналізованого процесу (рис. 19).

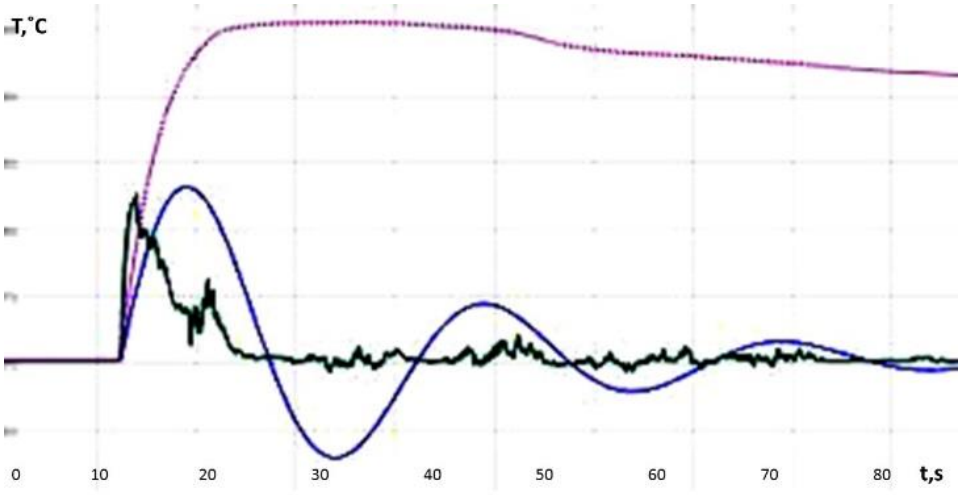


Рисунок 19 – Моделювання САР для переходів від 90 до 120˚С.

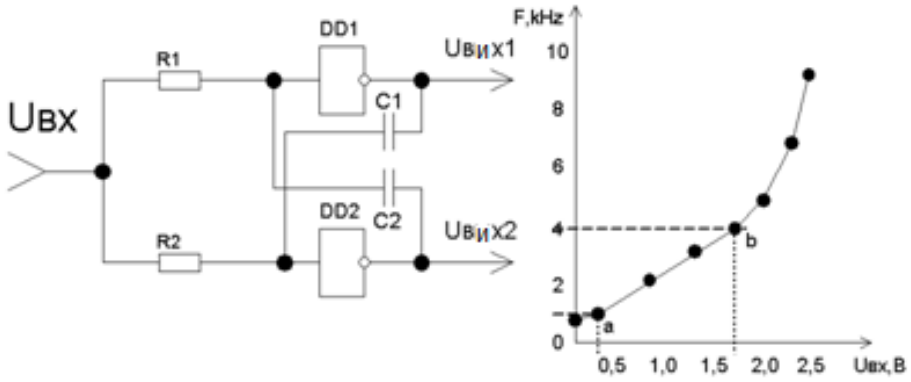
Аналіз системи теплоавтоматики зі змінними налаштуваннями. На базі Matlab & Simulink for fuzzy logic Toolbox було створено модель системи керування з нечіткою логікою. Модель включала п’ять датчиків для контролю температури в різних частинах ЕМО.

Для вирішення завдання захисту інформаційних даних в умовах перешкод, враховувалася ефективна поведінка перетворювача «інформаційний сигнал – частота». На рисунку 20 представлений варіант модулятора для аналогового сигналу *Uвх* на виході датчика-перетворювача з рівнем напруги $U_{вх} = 0{,}27 \ldots 1{,}75$ *В*. При цьому досягається відповідний інтервал значень частот *Fi* інформаційних повідомлень *(Есаулов С. М., Бабичева О. Ф., Шавкун В. М., 2008)*.

Вибір інтервалу контрольованої ділянки кривої «a-b» експериментальної характеристики вимірювальної схеми обумовлений його лінійністю

$$F = f(U_{вх}), \tag{38}$$

що важливо враховувати, застосовуючи такий пристрій у будь-яких засобах автоматики.



Рисунку 20 – Найпростіший перетворювач «напруга – частота»:

R1, R2 – резистори, *C1, C2* – конденсатори; *DD1, DD2* – логічні елементи,

F – частота вихідного сигналу, Гц; *Uвх* – вхідна величина, В

Щоб створити надійний канал передачі вихідних даних від такого датчика, його оснащують додатковим стабільним опорним генератором низької частоти. Застосовуючи опорну частоту F_0 інформаційний вихідний сигнал у цьому випадку зручніше контролювати через параметр ΔF

$$\Delta F = Fi - F_0, \tag{39}$$

який і був прийнятий під час аналізу теплового стану компонента ЕМО.

Як зазначалося вище, при використанні тональної модуляції передачі параметричної інформації, доцільно передбачити вузькосмуговий фільтр нижніх частот для більш ефективної боротьби з можливими перешкодами. Реальна схема датчика-перетворювача може істотно відрізнятися від схеми на рисунку 20. Однак, розглянутий варіант перетворення вихідних даних

досить добре вивчений і при необхідності може бути завершений створенням прикладного варіанту придатного пристрою для використання з адекватною математичною моделлю процесу нагріву. Таке рішення придатне для електронного моделювання та програмування такого компонента САР із прикладною спрямованістю. Таке пропоноване технічне рішення з частотним компаратором можна покласти в основу синтезу дискретного аналізатора справності частин діагностованого обладнання при послідовному опитуванні датчиків, що зручно застосувати в мобільному варіанті такого приладу.

При програмуванні алгоритму роботи керуючого пристрою слід розглядати структуру з використанням звукової карти. Це полегшує розробку локального спектрографа на базі ноутбука або планшета. У цьому слід враховувати інтервал частот, що лінійно взаємопов'язані з контрольованим параметром (ділянка «a – b», рис. 20). В експериментальному варіанті запропонованого рішення інформаційний сигнал на екрані інтерфейсу монітора представлявся користувачеві у вигляді монохромних ліній від усіх джерел сигналів, що використовуються. Приклад інтерфейсу такого пристрою на екрані ноутбука ілюструє рисунок 21.

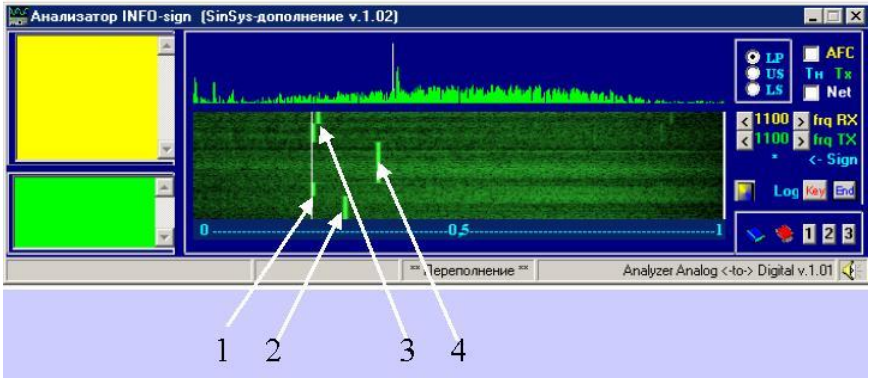


Рисунок 21 – Інтерфейс аналізатора з індикацією контрольованих величин: 1 – опорний сигнал; 2 – 4 – контрольований сигнал при варіюванні вимірюваної величини

Рядкове відображення поточного параметра на рисунку 21 ілюструє можливості аналізованого аналізатора, який дозволяє досить ефективно реєструвати зміну частоти контрольованої величини щодо опорної частоти (1) відповідно на 10 Гц (3), 100 Гц (2), 200 Гц (4) і т.д., що публікуються відповідними табло для користувача.

Прилад з такою візуалізацією дозволяє контролювати декілька десятків параметричних величин одночасно. Для підвищення селективності приладу для ідентифікації можливих несправностей доцільно виконати тимчасове рознесення інформації від датчиків або активувати на екрані тільки датчики з небезпечними величинами контрольованого параметра. Для таких рішень придатні будь-які таймери та нормувальники сигналів, що виділяють лише небезпечні рівні частот вимірювальних сигналів.

Під час програмування САР можна передбачити аналіз інформаційних сигналів за величиною $\Delta F = f(F - F_0)$. У цьому випадку гранично-допустимі значення можна застосувати для формування сигналів оповіщення та тривоги, публікації коротких словесних повідомлень у відповідному місці інтерфейсу тощо.

Щодо використання класичного ПІД-регулятора в САР слід враховувати, що він повинен містити три вбудовані датчики контролю вихідних сигналів схеми, що формує величини *Kp, Ki, Kd*. Ці величини необхідні реалізації блоку НАУ.

Використовуючи експериментальні дані значень всіх уставок ПІД-контролера, була обрана система вхідних функцій, при яких визначалася логіка формування вихідних величин, що реалізує прописані правила перемикання та зміни передбачених режимів. Як базовий варіант використовувався комплект САР з класичним ПІД-контролером.

При розробці блоку НАУ (рис. 22) використовувалися дані експериментів із багаторівневими трикутними та Гаусовими функціями. Вибір обумовлений можливістю дискретно або плавно змінювати режими зміни параметрів налаштування регулятора.

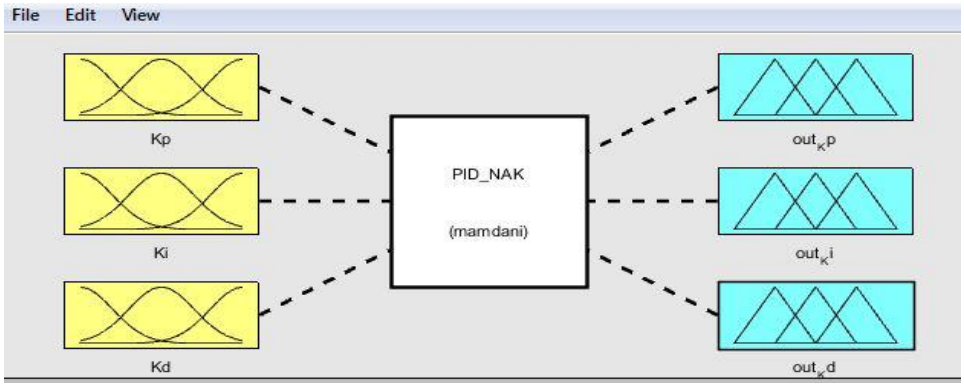


Рисунок 22 – Стартова страниця Fuzzy logic Designe

Вихідний проект блоку НАУ виконувався за допомогою Control System Toolbox пакета Matlab. Для налаштування FIS застосовувалася поверхня управління від вхідних параметрів до виходу з урахуванням проектних рішень *(Chen J., Huang T., 2004)*. Нормування значень вхідних величин виконувалося в інтервалі (–5; 5) з використанням вхідних функцій приналежності, які перекривали сусідні функції значення 0,5. Такий вибір змінних дозволив задавати вихідні функції приналежності. Нечіткі правила формувалися як:

1. IF ‘Помилка’ IS ‘ПомилкаНегативна’ THEN ‘Вплив’ IS
‘Зменшити’.
2. IF ‘Помилка’ IS ‘ПомилкаПозитивна’ THEN ‘Вплив’ IS
‘Збільшити’
3. IF ‘Інтеграл’ IS ‘ІнтегралНегативний’ THEN ‘Вплив’

IS ‘Зменшити’.

4. IF ‘Інтеграл’ IS ‘ІнтегралПозитивний’ THEN ‘Вплив’

IS ‘Збільшити’.

5. IF ‘Похідна’ IS ‘ПохіднаНегативна’ THEN

‘Вплив’ IS ‘Зменшити’.

6. IF ‘Похідна’ IS ‘ПохіднаПозитивна’ THEN

‘Вплив’ IS ‘Збільшити’.

На рисунку 23 ілюструється фрагмент комплекту правил експериментального блоку НАУ.

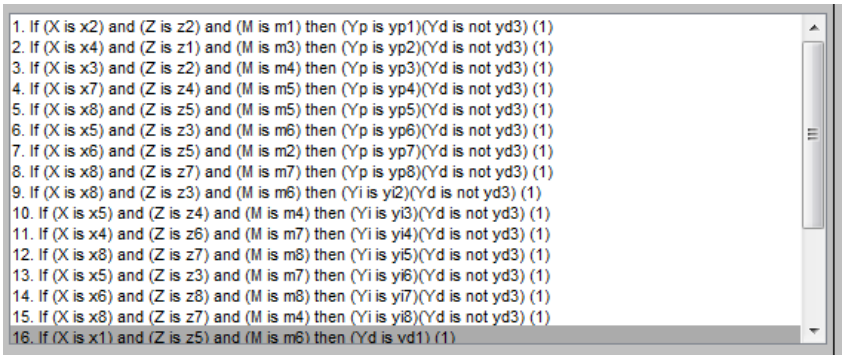
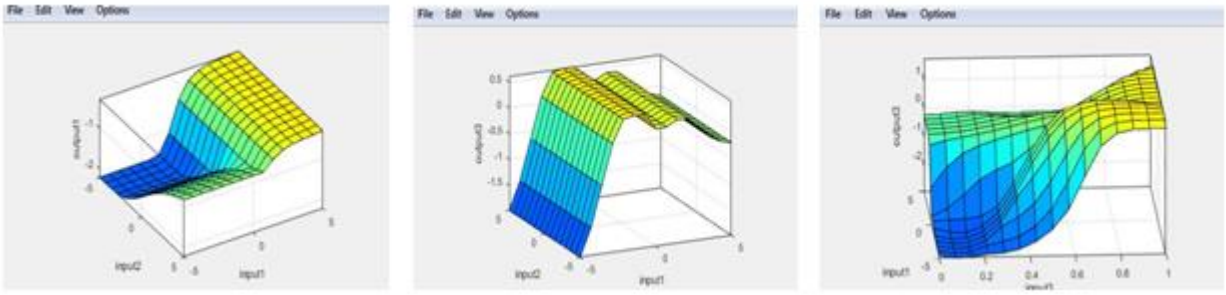


Рисунок 23 – Вікно фрагмента редактора правил для НАУ

Редактор правил, що застосовується, дозволяє виконувати візуалізацію нелінійних поверхонь, що відображають управління всіма змінними, вибір яких вказує на можливість зміни помилки регулювання. Якщо помилка має тенденцію до зменшення, ефективність процесу пошуку вихідних величин можна підвищити, застосувавши оновлення вихідних даних в інтерполяційній таблиці. При реалізації цього процесу доцільно передбачити запам’ятовування та вибірку середніх значень поточних величин у точках контролю температури на конкретному об’єкті керування.

Окремі графічні фрагменти бази правил для даного пристрою представлені на рисунку 24. Усі інтерпретації вихідних сигналів мали змінний характер, але за їх допомогою можна зробити певні висновки.



Рисунку 24 – Фрагменти графічних інтерпретацій вихідних сигналів блоку фазифікації

Оскільки набір правил створюється за допомогою дослідних даних, будь-яке правило легко перевірити, користуючись, наприклад, двоканальним осцилографом. Зручність візуального аналізу обумовлена також можливістю контролю та порівняння вихідних сигналів у варіантах класичного ПІД- і з нечітким блоком НАУ регуляторах. При задовільній згоді результатів вимірювань компоненти, що реалізують нечітку логіку, зручно представити бібліотекою даних у додатковому мікроконтролері, що включає не менше 8 портів введення вихідних даних і не менше 3 аналогових виходів. Зважаючи на характеристики популярних мікроконтролерів Arduino, у цьому сімействі є зразки, що відповідають зазначеним вимогам. Наприклад, мікроконтролери ATmega328 або ATmega32U4 з робочою напругою 5 В характеризуються такими параметрами: напруга живлення 6 –20 В; цифрових входів/виходів 14; аналогових виходів 6; максимальний струм кожного виходу 40 мА; максимальний вихідний струм виведення 3,3 може досягати 50 мА; Flash-пам'ять 32 Кб (SRAM 2 Кб; EEPROM 1 Кб; тактова частота 16 МГц) *(Arduino as ISP)*. Враховуючи реальні швидкості обробки вихідних даних і розрахункових величин, тактова частота менше 20 МГц у вибраному мікроконтролері цілком придатна для реалізації прикладних задач.

У запропонованій системі автоматики передбачаються вихідні сигнали підключення виконавчих механізмів. Активація аналого-дискретних приводів вентилятора та жалюзі припливного повітроводу повинні забезпечувати заданий приплив та відбір теплоносія під час роботи обладнання. На основі експериментів можна зробити висновок, що привод жалюзі придатний для реалізації малих, а вентилятори – для великих значень коефіцієнтів посилення виконавчого механізму.

Окрім відповідності вимог компонентів блоку НАУ з представленими вище технічними характеристиками, враховувався також змінний характер динамічних властивостей розглядуваного об'єкта управління, стохастичний характер яких обов'язково спричинить безперервність пошуку уставок *Kp, Ki, Kd*. Щоб виключити такий небажаний режим роботи, доцільно обмежити інтервали температури, для яких дискретно повинен виконуватися пошук шуканих величин уставок з обов'язковим запам'ятовуванням вихідних даних від усіх датчиків контролю до завершення налаштування ПІД-регулятора відповідного контуру регулювання. Як показали експерименти, вимушена зупинка САР під час пошуку уставок може тривати від часток до кількох секунд, але такі нетривалі тимчасові паузи за командою "STOP" найчастіше на результатах роботи комплекту ПІД&НАУ не мають негативного впливу, тому що теплові процеси відрізняються суттєвою інерційністю.

Також, якщо мимовільні процеси охолодження обладнання (рис. 11) можна визнати задовільними, то розробки НАУ для управління такими подіями можна створювати автономний контур управління процесом охолодження. Однак у холодильному обладнанні такий контур

управління процесом охолодження обов'язково передбачається. Вочевидь, що доцільність синтезу багатоконтурної системи управління з автономними блоками фазифікації як при нагріванні, так і при охолодженні компонентів ЕМО завжди визначатиметься розробником.

Експериментально встановлено, що на реалізацію правил витрачаються невисокі обчислювальні ресурси, тому що відстежуються лише рівні перегріву обладнання. Якщо виникає нестача об'єму Flash-пам'яті, що є в мікроконтролері, доцільно використовувати варіант з модулем для підключення SD карти Arduino. SD-модуль як зовнішній накопичувач може істотно збільшити пам'ять і багаторазово збільшити місце для зберігання корисної поточної інформації, що отримується в реальному часі. Знімний універсальний накопичувач SD є звичайною платою, на якій вміщено слот для карти, що має приблизно такі технічні характеристики: діапазон робочих напруг 4,5 – 5 В; підтримка карти SD до 2 Гб; струм 80 мА; Файлова система FAT 16) *(Talbi N., 2019).*

Оскільки запропоноване рішення спочатку потребує реальних вихідних даних та необхідність попереднього ретельного настроювання класичного ПІД-регулятора, то ці вимоги слід віднести до недоліків комплекту ПІД&НАУ, тому що реальну вибірку уставок можна отримати, експериментуючи з конкретним технологічним об'єктом. У таблиці 3 наведені результати експериментів із розглянутими комплектами ПІД-контролерів.

Таблиця 3 – Результати моделювання САР

Параметр оцінки	**ПІД-регулятор**	**ПІД&НАУ регулятор**
Перерегулювання нормованого перехідного процесу, %	0,9	1,7
Перерегулювання ненормованого перехідного процесу, %	28	4,6
Інтегральний показник якості, с	79	42
Тривалість перехідного процесу, с	91,15	36,62
Транспортне запізнення, с	12	12

До переваг запропонованого блоку фазифікації слід зарахувати: відсутність необхідності мати адекватну математичну модель керованого технологічного об'єкта; можливість мимовільного моделювання алгоритму функціонування на основі правил, що відповідають керованим подіям; можливість застосування додаткового каналу управління без взаємодії з основним ПІД-контролером, що здійснюється за допомогою додаткового виконавчого автономного пристрою. У такому разі зручно застосовувати виконавчі механізми з меншими коефіцієнтами посилення (привод жалюзі), ніж основний виконавчий пристрій (примусовий вентилятор охолодження).

Зазначений аналіз може бути привабливим розробки інтелектуальних системи автоматики з урахуванням вже функціонуючої системи з традиційним ПИД-регулятором.

У таблиці 4 наведені експериментальні дані моделі комплекту блоку фазифікації, що формує електричні величини *UKп, Uкі, UKд* з нормованим рівнем вихідного сигналу до 5 В. При цьому підстроювальні коефіцієнти *UKp, UKi, UKd* від *Kp, Ki, Kd* приблизно визначалися такими рішеннями:

$$U = 5; \tag{40}$$

$$UKp = U\cdot(Kp-sqrt(Rp\hat{}2-4\cdot Ki\cdot Kd))/2/Ki; \tag{41}$$

$$UKi = Ki/U; \tag{42}$$

$$UKd = Kd/Ukp. \tag{43}$$

Таблиця 4 – Результати автоматичного формування коригувальних сигналів блоком НАУ

Температурний нагрів, ˚С	**Настроювальні параметри ПІД**			**Вихідні сигнали НАУ**			**Характеристика вихідного сигналу**
	Kp	***Ki***	***Kd***	***UKp, В***	***UKi, В***	***UKd, В***	
60	12	$1{,}7\cdot10^{-4}$	11,7	3,11	1.210	2,7	нестабільний
80	12	$1{,}7\cdot10^{-4}$	11,7	4,10	1.105	0,6	монотонний
90	12	$1{,}7\cdot10^{-4}$	11,7	3,52	2.035	1,9	монотонний
100	37	$29{,}7\cdot10^{-4}$	0,7	4,72	3.045	2,9	нестабільний
110	37	$29{,}7\cdot10^{-4}$	0,7	3,81	2.225	2,4	нестабільний
120	26	$29{,}7\cdot10^{-4}$	0,7	4,39	3.305	0,4	монотонний

Зазначена в таблиці 4 нестабільність вихідного сигналу блоку НАУ, обумовлена невисокою стійкістю до перешкод електронної схеми, що формує сигнал $U_{Кд}$. Оскільки немає систем автоматики, які б переважали над аналогічними рішеннями за всіма показниками, то вибір розглянутої архітектури комплекту керуючого пристрою із застосуванням ПІД-контролером може привернути до себе увагу розробників, орієнтованих на технологічний регламент та економічне забезпечення апаратного оформлення процесу. Очевидно, що в кожному випадку розробник переслідуватиме такий шлях, який спричинить покращення роботи окремих компонентів, що формують, наприклад, у блоці фазифікації, керуючі величини, адекватні подіям у реальному об’єкті *(Єсаулов С. М., Хворост М. В. , Бабічева О. Ф. , Найдьонов М. О., 2023).*

Висновки. Використовуючи аналітичні та експериментальні дані процесу нагрівання експлуатованого електромеханічного обладнання (ЕМО), був вивчений взаємозв’язок параметрів та причин стохастичного тепловиділення окремими частинами.

1. Вивчений тепловий контроль подій в ЕМО за допомогою вимірювального пристрою на базі датчика-перетворювача «температура-частота».

2. Експериментальна реалізація та аналітичний опис робочого циклу ЕМО виявили можливість застосування регресійної математичної моделі для отримання теплових варіативних інтервалів придатних для діагностики можливих неполадок у типовому обладнанні електричного транспорту.

3. Виконано дослідження експериментального комплекту аналогово-цифрового візуального аналізатора тональних інформаційних сигналів від кількох термодатчиків, які підтвердили можливість використання таких пристроїв для дистанційної теплової діагностики справності компонентів ЕМО.

4. За допомогою програмного середовища Matlab&Simulink виконано моделювання та ілюструються результати досліджень систем стабілізації теплового режиму ЕМО із застосуванням класичного та нечіткого ПІД-регуляторів для об'єкта зі змінними динамічними властивостями.

5. Подані результати досліджень виявили переваги та недоліки САР з ПІД-регулятором, що містить блок нечіткого алгоритму управління налаштувань параметрів, що реалізують певний закон регулювання для досягнення найбільшого узгодження керуючих величин з реальними подіями в об'єкті управління.

References:

Квасніков В. П., Квашук Д. М., Катаєва М. О. Розробка стенду для вимірювання метрологічних характеристик електродвигунів. *Aerospace technic and technology*. 2021. P. 104–111. DOI:10.32620/aktt.2021.4sup2.14

Афанасов А. М. Розвиток наукових основ та вдосконалення енергоефективних методів випробування тягових електричних машин постійного та пульсуючого струму: автореф. дис… д-ра техн. наук: 05.22.09, 05.22.12. Дніпропетровськ, 2013. 39 с.

Квасніков В. П., Квашук Д. М., Катаєва М. О. Розробка інформаційно-вимірювальної системи діагностики робочих характеристик електродвигунів. *Збірник наукових праць Одеської державної академії технічного регулювання та якості*. Вип. 1(18). С. 42–52. DOI: 10.32684/2412-5288-2021-1-18-42-52

Бондар Б. Є., Очкасов О. Б., Черняєв Д. В., Шевченко І. Я. Діагностування тягових електродвигунів за нерівномірністю обертання якоря. Наука та прогрес транспорту. 2013. Вип. 3(45). С. 13 – 21

Есаулов С. М., Бабичева О. Ф., Шавкун В. М. Проектирование эталонной модели для системы диагностирования оборудования на транспорте. Восточно-европейский журнал передовых технологий. Вып.6/2(36). 2008. С. 39 − 42.

Есаулов С. М., Бабичева О. Ф., Лукашова Н. П. Проектирование компонентов для систем автоматического диагностирования транспорта. Восточно-европейский журнал передовых технологий. Вып.5/3(41). 2009. С. 28 − 32

Gunal S., Gokhan Ece D., Gerek O.N. Induction machine condition monitoring using notchfiltered motor current. *Mechanical Systems and Signal Processing*. 2009. Vol. 23, iss. 8, pp. 2658 – 2670. DOI:10.1016/j.ymssp.2009.05.011

Єсаулов С. М., Бабічева О. Ф., Акіньшин Д. О. Синтез компонентів теплового діагностичного експерта зі штучним нейроном. *Комунальне господарство міст: Серія: Технічні науки та архітектура. Наук.-техн. сб.* – Харків: ХНУМГ, 2021. Том 1, № 161 (2021). С. 148 – 156. DOI: 10.33042/2522-1809-2021-1-161-148-156

Deuszkiewicz P., Radkowski S. On-line condition monitoring of a power transmission of a rail vehicle. *Mechanical Systems and Signal Processing*.Volume 17. Issue 6. 2003. P.1321 – 1334. DOI: 10.1006/mssp.2002.1578
Єсаулов С. М., Бабічева О. Ф., Ковалик М. М. Контроль і моделювання параметрів для теплової діагностики порушень силового електрообладнання. *Комунальне господарство міст: Наук.-техн. сб.* Харків: ХНУМГ, 2019. Вип. 3(149). С. 19-28 DOI: 10.33042/2522-1809-2019-3-149-19-28
Szymański, Z. Diagnostic model of the wheel vehicle drive system based on FEM, BEM, and random system. *Proceedings of ISEF'09* (10 September – 12 September 2009). Arras, 2009. P. 183–193 DOI:10.3233/978-1-60750-604-1-183
Єсаулов С. М., Бабічева О. Ф., Ковалик М. М. Підвищення ефективності теплового діагностичного контролю справності електродвигунів. *Комунальне господарство міст: Серія: Технічні науки та архітектура*. Наук.-техн. сб. Харків: ХНУМГ, 2020. Том 4. № 157 (2020). С. 163 – 171. DOI: 10.33042/2522-1809-2020-4-157-163-171
Yesil E.; Guzelkaya M.; Eksin I. Internal model control based fuzzy gain scheduling technique of pid controllers. *World Automation Congress,*. Proceedings. Vol. 17, 28 June – 1 July 2004, p. 501 – 506. DOI:10.1109/WAC.2004.185457
Єсаулов С. М., Бабічева О. Ф., Рогожина Х. О. Дослідження, моделювання і проектування компонентів штучного нейромережевого модуля для дистанційної діагностики електродвигунів. Комунальне господарство міст. К. : Техніка. Вып.5(151). 2019. С. 13 – 22 DOI: 10.33042/2522-1809-2019-5-151-13-22
Sabri, Laith & Al-mshat, Hussein. Implementation of Fuzzy and PID Controller to Water Level System using LabView. *International Journal of Computer Applications*. 2015. № 116. P. 6 – 10. http://dx.doi.org/10.5120/20378-2599
Єсаулов С. М., Хворост М. В. , Бабічева О. Ф. , Найдьонов М. О. Застосування нечіткої логіки в системі керування електромеханічним обладнанням. *Комунальне господарство міст. Науково-технічний збірник*. Том 6 №180 (2023). С. 33 – 42 https://doi.org/10.33042/2522-1809-2023-6-180-33-42
Astrom K. J. Advanced PID control / K. J. Astrom, T. Hagglund. – Research Triangle Park, NC (USA) : ISA – The Instrumentation, Systems, and Automation Society, 2006. – 460 p. – Regime of access: https://lib.ugent.be/catalog/rug01:001975694,
MATLAB. The Language of Technical Computing. Getting Started with MATLAB. *The Math Works, Inc. USA*. 2000. URL: http://www-eio.upc.es/lceio/manuals/matlab/TECHDOC/PDFDOCS/GETSTART.PDF
Talbi N. Design of Fuzzy Controller rule base using Bat Algorithm. *Energy Procedia*. 2019. Vol. 162, P. 241 – 250. DOI:10.1016/j.egypro.2019.04.026
Arduino as ISP and Arduino Bootloaders I Arduino Documentation URL: https://docs.arduino.cc
Chen J., Huang T. Applying neural networks to on–line updated PID controllers for nonlinear process control. *Journal of Process Control*. 2004. №14. P. 211 – 230. https://doi.org/10.1016/S0959-1524(03)00039-8

DOI 10.5281/zenodo.10822025
UDC 351.746:007

CHAPTER 18.
FEATURES OF THE STATE POLICY REGARDING THE FORMATION OF THE INFORMATION SECURITY IN THE CONDITIONS OF DIGITALIZATION

Valentyn DIACHENKO
Candidate of Economic Sciences,
Associate Professor of the Department of Cybersecurity, IT and Economics,
Kyiv University of Intellectual Property and Law, National University "Odesa Law Academy"
(210, Kharkiv highway, Kyiv, 02121 Ukraine)
dyachenko v@ukr.net
https://orcid.org/ 0000-0002-0055-9256

Nataliia DIACHENKO
Candidate of Sciences in Public Administration,
Associate Professor of the Department of Cybersecurity, IT and Economics,
Kyiv University of Intellectual Property and Law, National University "Odesa Law Academy"
(210, Kharkiv highway, Kyiv, 02121 Ukraine)
n.diachenko@ukr.net
https://orcid.org/0000-0002-4306-7665

Abstract. The urgency of the need to find mechanisms for improving state policy regarding the formation of the information security in the conditions of the digitalization determined the direction of the research. Trends in the introduction of the information technologies into the educational process of the higher education institutions have been revealed. The priority directions for improvement of the educational components have been identified. It was emphasized that higher education institutions, taking into account modern trends and future needs on the labor market, in particular during post-war reconstruction, need to involve highly qualified practitioners in their teaching activities to ensure the level of the information technology teaching, in accordance with modern standards, requirements of professional activity, needs forming the foundations of the information and national security and the needs of the society. It is emphasized that the information component of the public administration mechanisms is a basic factor in the effectiveness of the public

administration, because in the conditions of hybrid threats and the need for systematic protection of the information in cyberspace, the issue of the operational information support for the processes of the forming management decisions, including in the field of the public administration, is extremely relevant. The need for access to operational, true and impartial information in the conditions of the martial law determines the need to modernize the state information policy, which is carried out on the basis of the web technologies that ensure the interactive nature of the digital communications.

Keywords: information technologies, information communication and digital technologists, IT sphere, information security.

ОСОБЛИВОСТІ ДЕРЖАВНОЇ ПОЛІТИКИ ЩОДО ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ

Анотація. Актуальність потреби пошуку механізмів удосконалення державної політики щодо формування інформаційної безпеки в умовах діджиталізації обумовили напрям дослідження. Виявлено тенденції впровадження інформаційних технологій у навчальний процес закладів вищої освіти. Виявлено пріоритетні напрями удосконалення освітніх компонентів. Наголошено, що закладам вищої освіти, з урахуванням сучасних тенденцій, майбутніх потреб на ринку праці, зокрема й при повоєнній відбудові, необхідно до викладацької діяльності залучати висококваліфікованих фахівців-практиків для забезпечення рівня викладання інформаційних технологій, відповідно до сучасних стандартів, вимог професійної діяльності, потреб формування засад інформаційної та національної безпеки й потреб суспільства. Акцентовано, що інформаційна складова механізмів публічного адміністрування є базовим чинником ефективності державного управління, адже в умовах гібридних загроз та необхідності системного захисту інформації у кіберпросторі, питання оперативного інформаційного забезпечення процесів формування управлінських рішень, у тому числі й у сфері публічного управління, є надзвичайно актуальним. Потреба у доступі до оперативної правдивої та неупередженої інформації в умовах воєнного стану обумовлює потребу модернізації державної інформаційної політики, що здійснюються на основі web-технологій, які забезпечують інтерактивний характер digital-комунікацій.

Ключові слова: інформаційні технології, інформаційно-комунікаційні та цифрові технологі, ІТ-сфера, інформаційна безпека.

ВСТУП. Упровадження нових стандартів вищої професійної освіти обумовлює потребу змін цілей, технологій та результатів освітньої діяльності. В умовах формування засад інформаційного суспільства та діджиталізації, як каталізатора інноваційного суспільного та економічного розвитку, гостро постає потреба підготовки кваліфікованих фахівців у сфері

інформаційних технологій. Питанням аналізу рівня підготовки спеціалістів у сфері інформаційно-телекомунікаційних технологій, у тому числі й у країнах ЄС, та особливостям формування інформаційно-комунікаційної компетентності у здобувачів вищої освіти приділили увагу ряд науковців, які наголошують, що інформаційно-комунікаційна компетентність у здобувачів вищої освіти, як підтверджена на практиці здатність особистості на основі опанованих знань, умінь та навичок використання ресурсів хмарних технологій, формує передумови використання таких технологій для задоволення власних індивідуальних, у тому числі й навчальних, потреб і розв'язування професійних задач у майбутньому *(Спірін О., Вакалюк Т., 2019)* та, зокрема, пропонують виокремити інформаційно-обчислювальну компетентність майбутніх фахівців як спеціальну компетентність з інформаційних технологій *(Капітон А., 2023)*, яку необхідно формувати у здобувачів вищої освіти протягом усіх років навчання в закладі вищої освіти.

Ряд науковців рекомендують формувати у здобувачів вищої освіти репродуктивний та адаптивний рівні оволодіння цифровою компетентністю шляхом опанування теоретичними знаннями, вміннями та практичними навичками використання інформаційно-комунікаційних технологій у процесі навчання *(Abysova M., Kravchuk M., Hurniak O., 2023),* та наголошують, що використання хмарних технологій в умовах онлайн навчання є ефективним *(Pokhre S. ma Chhetri R., 2021),* бо не лише надає можливість продовжувати навчальний процес, а й, завдячуючи можливості скористатись хмарними технологіями та комп'ютерними інструментами, інтенсифікувати процес отримання знань, умінь та практичних навичок здобувачами вищої освіти.

S. Bamforth, G. Perkin, J. Flint описують переваги використання, зокрема на планшетному комп'ютері, де присутня можливість рукописного введення тексту та додавання нотаток, Microsoft Office OneNote. Microsoft Office OneNote – застосунок для створення нотаток та систематизації особистої інформації від корпорації Microsoft *(Bamforth S., Perkin G., Flint J., 2019)*, що є частиною пакету Microsoft Office та наполегливо рекомендують формувати у здобувачів вищої освіти soft skills (укр. м'які/гнучкі навички), які, відповідно до дослідження, ефективно сприяють опануванню знаннями, необхідними у подальшій професійній діяльності *(R. Lavi, M. Tal ma Y. Dori, 2021).*

Ряд науковців, визначаючи хмарні технології як повний, зручний мережевий доступ за вимогою інтернету до численних інтернет-ресурсів (наприклад, мереж, серверів, сховищ, програм і послуг), які можна швидко знайти, до яких можна легко, з мінімальними зусиллями по управлінню або взаємодії з постачальником послуг, приєднатись чи вийти

(Polyviou A., Venters W., Pouloud N., 2023), виокремлюють серед передбачуваних переваг їх використання такі:

– хмарні послуги, за умови наявності доступу до мережі інтернет, можуть надаватися не залежно від географічного положення користувача;

– відсутність потреби безпосередньої взаємодії з постачальником послуг;

– інтенсифікація процесу пошуку необхідної оперативної інформації, коригування запиту та консолідація наявної інформації.

Кіберпереслідування, кіберзалякування, кібертероризм, кіберзлом, витік даних, крадіжка особистих даних, фішинг та інші види кіберпереслідувань постійно відбуваються у віртуальному світі. Зазначаючи, що кіберзлочинці використовують наперед визначені комп'ютерні програми та заздалегідь скореговані плани, а кіберпереслідування та кіберзалякування майже близькі за змістом та намірами, адже при їх здійсненні використовуються одні й ті ж самі інтернет-технології для переслідування, залякування та підриву інтересів інших людей в Інтернеті, науковці наголошують, що саме знання методів своєчасного виявлення ознак кіберпереслідувань та практичні навички по їх нейтралізації, набуті у процесі «машинного навчання» формують підґрунтя для інформаційної та кібернетичної безпеки *(Gautam A., Bansal A., 2022),* загалом, *(Novachenko T., Bielska T, Afonin E, 2020)* використання інформаційних технологій сприяє не лише підвищенню економічної ефективності а й, шляхом надання оперативного доступу до публічної інформації, формує засади зростання довіри у суспільстві.

Саме потреба дослідження механізмів удосконалення викладання освітніх компонентів сфери інформаційних технологій з урахуванням тенденцій їх розвитку, особливостей їх упровадження у різні сфери суспільного життя та з огляду на сьогоденні виклики обумовлюють потребу модернізації освітнього процесу.

Глобальні тенденції впливу на майже на всі процеси суспільного буття зумовили перехід світового суспільства до наступної стадії розвитку – глобального інформаційного суспільства, в якому, інформація – це стратегічний ресурс трансформаційних змін в суспільстві.

Україна у 2022 році задає тренди з відкриття даних, адже поділяє першість в Європі разом з Кіпром, Данією, Естонією, Ірландією, Італією, Польщею та Іспанією *(Open Data Maturity, 2022)*. І ця тенденція зберігається вже другий рік поспіль.

За версією Всесвітньої організації інтелектуальної власності (англ. WIPO), Україна – серед найбільш інноваційних країн – 49 місце *(Global Innovation Index, 2022),* а Національна система освіти України готує суттєву, у порівнянні з іншими країнами, кількість фахівців інформаційно-комунікаційних технологій (далі – ІКТ) для ІТ-сфери (табл. 1):

Таблиця 1.

Кількість здобувачів вищої освіти ІКТ та кількість випускників ІКТ

	Кількість студентів ІКТ, *тис.осіб*	Кількість випускників ІКТ, *осіб на 100 тис. осіб населення*
Україна	104,7	68,0
Польща	50,3	23,0
Сербія	22,5	46,0
Угорщина	22,4	31,0
Словаччина	6,9	32
Литва	6,4	31,0
Естонія	4,4	54,0

Передові позиції у сфері підготовки фахівців інформаційно-комунікаційних технологій сприяють підвищенню рівня обізнаності громадян та обумовлюють потребу забезпечення якості викладання прикладних освітніх компонентів у закладах вищої освіти, зокрема шляхом використання інтерактивних моделей навчання, адже організація сучасного освітнього процесу у закладах вищої освіти повинна сприяти задоволенню потреби здобувачів вищої освіти у творчій самореалізації, та інтелектуальному самовдосконаленню шляхом безперервного розвитку особистості.

У сучасних умовах воєнного стану в Україні особливо гостро постає потреба своєчасного отримання, систематизації, узагальнення інформації, її консолідації, формування оперативних управлінських рішень, стратегічних передбачень та надання послуг громадянам, що надзвичайно важливо, внутрішньо переміщеним особам, що й актуалізує потребу підготовки фахівців у сфері ІКТ.

Система національної вищої освіти в Україні традиційно виступає одним з базових чинників сталого державного розвитку, адже, готує фахівців, розвиває особистість, формує засади життєвої позиції. Упровадження інноваційних технологій в освітні процеси сприяє підготовці фахівців відповідно до вимог європейських та національних стандартів вищої освіти, сформованості ринку послуг, динамічного оновлення стандартів та потреб суспільства.

Сучасні педагогічні технології, що інтегруються з ІКТ сприяють формуванню у здобувачів вищої освіти високого рівня знань, вміння оперування інформацією, креативного та творчого мислення, комунікативних навичок, розширюють можливості для їх самоосвіти.

В Україні базові питання правових відносин щодо захисту інформації в автоматизованих системах врегульовуються з 1994 року *(Закон України, 1994)* і по теперішній

час, водночас, з урахуванням актуальних викликів та загроз гостро постає потреба захисту національних інформаційних ресурсів, як складової інформаційної безпеки України. На період дії правового режиму воєнного стану деякі конституційні права громадян щодо доступу до публічної інформації обмежено.

Результатом традицій останніх десятиліть щодо підготовки фахівців у сфері ІКТ технологій є усталена тенденція того, що інформаційні технології в Україні – провідний напрямок надання експортних послуг, навіть за умов воєнного стану, при якому за межі держави виїхали 57 000 спеціалістів. Водночас, навіть за таких екстремальних умов, 80% ІТ спеціалістів залишились в Україні, 2,5 % з них – у лавах Збройних Сил України *(Тарасовський Ю., 2022)*.

У зв'язку з виїздом за кордон частини спеціалістів в ІТ галузі, на ендогенному ринку ІТ-праці з'явились додаткові вакансії, так у місті Києві станом на 28 лютого 2024 року їх 1992 *(Work.ua, 2024)*, що на 23,3 % більше ніж 18 липня 2023 року, однак, умови передбачають наявність стажу у даній сфері щонайменше 2 роки, тому світчерам, як спеціалістам інших галузей, що отримали знання чи освіту з ІТ, набагато складніше працевлаштуватись, їх наразі більше ніж вакансій. Динаміка збільшення кількості вакансій спеціалістів в ІТ-сфері вказує на потребу збільшення чисельності здобувачів, у тому числі й вищої освіти, здатних у майбутньому працювати у сфері інформаційних технологій.

Актуальним напрямом диверсифікації діяльності у сфері інформаційних технологій є ефективне їх використання при проєктуванні, модернізації та розробці систем сучасного програмного забезпечення дронів.

У 2022 році український ринок дронів-обприскувачів став №1 у Європі *(Рубрика, 2022)*. Зростає попит на дрони у сільському господарстві, дронами-обприскувачами у 2022 році обробили 1,2 млн га, що на 20 % більше, ніж у попередньому році. Такі тенденції збережуться й у 2023 році, адже, для обслуговування дронів необхідно майже у двадцять разів менше пального та води та майже на 30 % препарату при внесенні пестицидів у порівнянні з наземною технікою. Важливою перевагою при використанні дронів у сільському господарстві є уникнення пошкодження рослин при їх обприскуванні.

Розширення сфери використання дронів сприяє формуванню додаткових робочих місць, зокрема завдяки експлуатації дронів-обпирскувачів у 2021 році, створено понад 1 тис. робочих місць в аграрних регіонах України. А відтак, необхідно розширити перелік освітніх компонентів для здобувачів вищої освіти галузі інформаційні технології, зокрема збільшити обсяги на викладання теорії з обслуговування дронів (безпілотних літальних апаратів).

Базовим напрямом диверсифікації діяльності у сфері інформаційних технологій став актуальний у часи воєнного стану національний Military Tech, актуалізований у 2014 році та вкрай необхідний наразі для створення та обслуговування, зокрема, сил проти повітряної оборони, автоматичних систем наведення та дронів.

У сфері стримування, оборони та наступу характерним є динамічний розвиток і застосування інформаційних комунікацій та технологій, у результаті яких з'явилось високоточне кероване озброєння, яке забезпечило, зокрема, й можливість ведення так званих мережевих воєнних дій.

Трендом безумовно є дрони – безпілотні літальні апарати (далі – БПЛА), за час воєнного стану взято на озброєння близько десятка вітчизняних БПЛА, зокрема, безпілотник E-300 Enterprice, дрон з корисним навантаженням у 300 кг, безпілотник D-80 Discovery дрон з корисним навантаженням у 80 кг *(Militarnyi, 2022)* та інші.

Такі тенденції вказують на зростаючу потребу у фахівцях інформаційних технологій, зокрема, й у лавах Збройних сил України.

У складних умовах правового режиму воєнного стану у 2022 році 93560 осіб було зараховано на навчання у заклади надання освіти різного рівня (рис. 1), що лише на 5,9% менше, ніж у 2021 році (99101 осіб), в якому на 85% збільшилась чисельність зарахованих, у порівнянні з 2020 роком (53437 осіб).

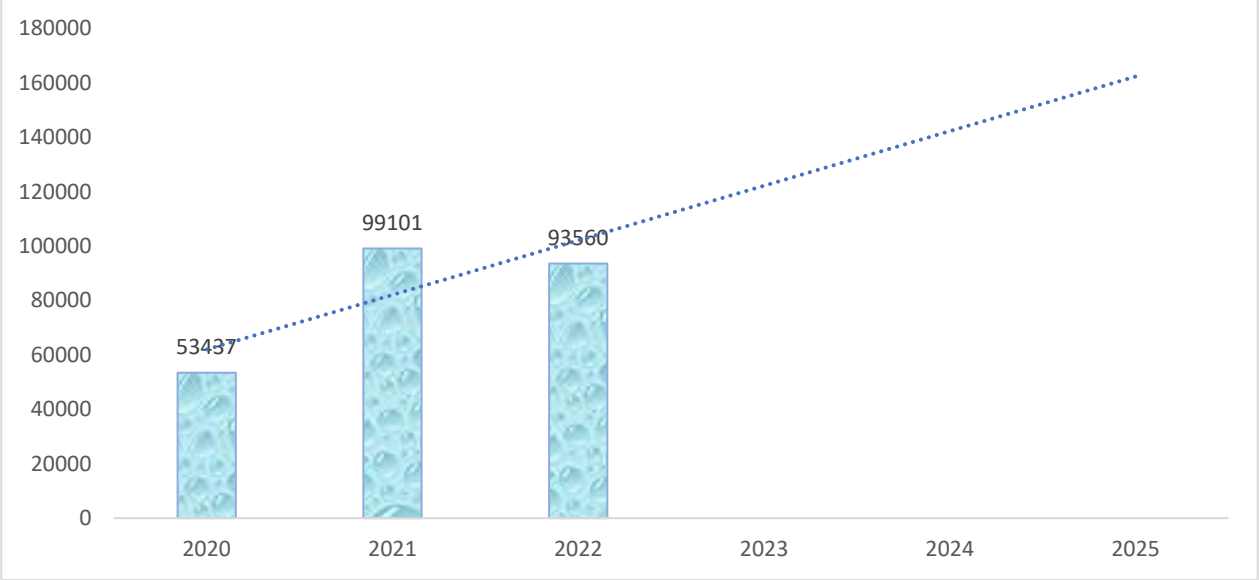


Рис. 1. Динаміка змін чисельності зарахованих осіб на навчання у заклади надання освіти різного рівня упродовж 2020-2022 років та тенденції тренду.

Джерело: Державна служба статистики України

Відповідно до лінії тренду маємо перспективи щодо зростання кількості бажаючих стати здобувачами вищої освіти у майбутньому.

Передумовою ефективності освітнього процесу у закладах вищої освіти є інформатизація навчального процесу, яка сприяє інтенсивності опанування здобувачами вищої освіти знань, умінь та практичних навичок, адаптації до сучасних стандартів їх майбутньої професійної діяльності та суспільного життя.

Важливими технологічною тенденцією сучасності є використання інформаційних технологій, що імітують реальність (від віртуальної та доповненої до змішаної), зокрема у сфері медицини, шоу-бізнесі та інших сферах.

Посеред технологічних трендів 2023 року варто виокремити:

– Розширену реальність (англ. Augmented reality, AR) – тренд, що об'єднує технології, які імітують реальність від віртуальної, доповненої чи змішаної. Технологія користується популярністю не лише у геймерів, а й у фахівців медичної сфери та багатьох сфер бізнесу, адже створює реальність без будь-якої матеріальної присутності.

– Граничні обчислення (англ. Edge Computing), які використовують для термінової обробки великий масивів даних. Суттєвою перевагою є можливість здійснювати операції з віддалених від офісів місць розташування.

– Блокчейн (англ. Blockchain), як технологія, яка передбачає лише доповнення попередніх блоків даних, що унеможливлює зміну даних чи їх вилучення, а, відтак, нівелюється потреба контролю чи перевірки за станом раніше внесеної інформації.

– Розумні пристрої (англ. Smart devices) – роботи зі штучним інтелектом покликані полегшити, зокрема, щоденну домашню працю та зробити наше життя комфортним *(Production Ready, 2023)*.

– Метавсесвіт (англ. Metauniverse), як надання можливостей віртуального шопінгу, віртуальних подорожей, віртуальної соціалізації, навчання VR чи промисловий метавсесвіт, більше відомий як Індустрія 5.0, що пропонує реальній економіці цифрову/віртуальну репрезентацію об'єктів, активів чи виробничих приміщень. Віртуальні офіси, які у часи пандемії та воєнного стану надали можливість продовжити діяльність компаніям, посприяли усуненню потреби оренди приміщення під офіс, а відтак, перетворили невизначеність на можливість для інноваційної діяльності. До 2027 року віртуальні робочі простори забезпечать 30 -ти відсоткове зростання інвестицій компаній у технології метавсесвіту *(Дяченко В., Дяченко Н., Голубков І., 2024)*.

У рамках інтерактивного та практико орієнтованого навчання здобувачів вищої освіти при опануванні ними інформаційно-телекомунікаційних технологій доцільно

використовувати кіберполігон – сукупність спеціальних програмно-апаратних комплексів, які об’єднані провідними та безпровідними засобами комунікацій, що можуть бути інтегрованими в мережу Інтернет та застосовуються для здійснення моніторингу впливу на системи управління, які можуть становити інтерес, для захисту власних систем від несанкціонованого доступу.

Навчальний кіберполігон сприяє формуванню у здобувачів вищої освіти системи професійних здатностей (рис. 2), адже дозволяє імітувати кібератаки, кібернапади на сервери, які обслуговують інфраструктури підприємства, установи чи організації для пошуку вразливих місць, усунення їх вразливості, налагодження ефективної системи захисту наявних комп’ютерних та інформаційно-комунікаційних ресурсів, відновлювати штатне їх функціонування.

Розгортання кіберполігону на базі закладу вищої освіти сприятиме набуттю ними навичок використання тактик передбачення кібератак, методів ідентифікації симуляції кібератак, відпрацювання методик їх відбиття, адже, програмне забезпечення та системи візуалізації сприяють відпрацюванню кібердій, що здійснюються у віртуальному середовищі. Системами візуалізації передбачено можливість моделювання кібератак, які можуть здійснюватись на комп’ютерні мережі, що передбачає зменшення чи й зовсім уникнення витрат на придбання ресурсів хмарних технологій *(Дяченко В., Дяченко Н., 2024)*.

Використання можливостей кіберполігону сприятиме формуванню у здобувачів вищої освіти здатності:

– використовувати програмні та програмно-апаратні комплекси засобів захисту інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах

– забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації усталеної політики інформаційної чи кібернетичної безпеки

– відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різного рівня та походження

– упроваджувати та забезпечувати функціонування комплексних систем захисту інформації, використовувати інформаційно-комунікаційні технології, сучасні методи та моделі інформаційної та/чи кібернетичної безпеки

– здійснювати професійну діяльність на основі впровадженої системи управління інформаційної та/чи кібернетичної безпеки

– застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності

– виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем відповідно до усталеної політики інформаційної чи кібернетичної безпеки

– аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційного простору та інформаційних ресурсів відповідно усталеної політики інформаційної чи кібернетичної безпеки

Рис. 2. Система професійних здатностей здобувачів вищої освіти при опануванні інформаційно-телекомунікаційних технологій з використанням кіберполігону

Набуті при опануванні можливостей кіберполігону здобувачами вищої освіти знання, вміння та практичні навички сприятимуть їх конкурентоздатності та затребуваності на вітчизняному ринку праці, а відтак забезпечать формування засад національної кібернетичної безпеки.

Актуальною наразі та затребуваною серед молоді та світчерів є потреба набуття знань з основ володіння комп'ютером, комп'ютерного програмування та кібербезпеки.

Базову інформацію такого формату безоплатно пропонує освітній проєкт «Go IT!», який пропонує вчити основи інформаційних технологій з нуля безкоштовно в онлайн форматі у стилі 7-ми денного марафону, допомагає світчерам увійти у сферу IT, пропонує роз'яснення чому саме у такі випробувальні часи правового режиму воєнного стану, саме IT-спеціалісти – це саме ті фахівці, які потрібні у всіх сферах життєдіяльності, зокрема й у сфері оборони.

Зацікавлює слухачів безкоштовними ознайомчими курсами також Online Institute Creative&Tech PTJCTR *(Online Institute Creative&Tech PTJCTR, 2024)*, девізом діяльності якого є «Освідчені – значить вільні». Менеджери інституту наголошують, що в IT-сфері є багато різних професій та пропонують спробувати IT професії на практиці.

Національна доктрина розвитку освіти обумовлює потребу у ході освітнього процесу створювати комфортні умови для самовизначення та самореалізації здобувачів вищої освіти.

Дієвим механізмом забезпечення зростання зацікавленості здобувачів вищої освіти у самостійному чи колективному пошуку інформації, її аналізі та знаходженні варіантів рішень поставленого викладачем завдання є використання інтерактивних методів навчання, які передбачають взаємонавчання здобувачів вищої освіти, групове чи колективне, де всі здобувачі та викладач є рівноправними суб'єктами навчального процесу.

Варто наголосити, що ігнорування потреби підготовки спеціалістів високої кваліфікації у сфері інформаційних технологій та їх відсутність на ринку праці створює для держави значні ризики. Відповідно дослідження, проведеного у 2023 році, *(Бондаренко О., 2023)* найбільш конкурентоспроможними виявляються ті держави, трудові ресурси яких максимально готові до використання інформаційно-телекомунікаційних технологій.

Публічний digital-маркетинг як елемент державної інформаційної політики

В умовах сучасного воєнного стану реалізація єдиної державної інформаційної політики є пріоритетним завданням національної безпеки, упровадження якої здійснюється, зокрема, шляхом об'єднання всіх загальнонаціональних телеканалів на єдиній інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні «Єдині новини» *(Єдині новини, 2022)*, метою якого є надання громадянам цілодобового доступу до оперативної достовірної інформації, чому певною мірою сприяє впровадження державної політики у сфері інформатизації – комплексу політичних, правових, економічних, соціально-культурних та організаційних заходів, спрямованих на встановлення загальнодержавних пріоритетів розвитку інформаційного середовища суспільства, що наразі формує підгрунтя для імплементації digital-комунікацій в системі публічного управління.

Загалом, про необхідність упровадження digital-маркетингу в систему публічного управління, свідчить зростання обсягу світового ринку цифрового маркетингу, який у

2022 році досяг майже 321 млрд доларів США. Очікується, що надалі ринок зростатиме із середньорічним темпом зростання 13,1% у період з 2023 по 2028 рік *(Global Digital Marketing, 2023)* і досягне до 2028 року близько 671,86 млрд доларів США. Водночас, зростає й загроза інтенсифікації проблем кібернетичної безпеки. А відтак, усі процеси у digital-маркетингу необхідно здійснювати відповідно до базових принципів кібернетичної безпеки, адже, персонал, який опікується питаннями digital-маркетингу, має доступ до стратегічно важливої інформації підприємства, установи чи організації. Саме тому, з метою збереження репутації, довіри користувачів та конкурентоздатності необхідно володіти знати інструменти та мати навички їх ефективного використання при управлінні еволюціонуючими ризиками кіберзагроз та шахрайства.

За версією Всесвітньої організації інтелектуальної власності (англ. WIPO), Україна є посеред найбільш інноваційних країн *(Global Innovation Index, 2022).*

Національна система освіти України готує суттєву, у порівнянні з іншими країнами, кількість фахівців інформаційно-комунікаційних технологій (далі – ІКТ) для ІТ-сфери (рис. 3):

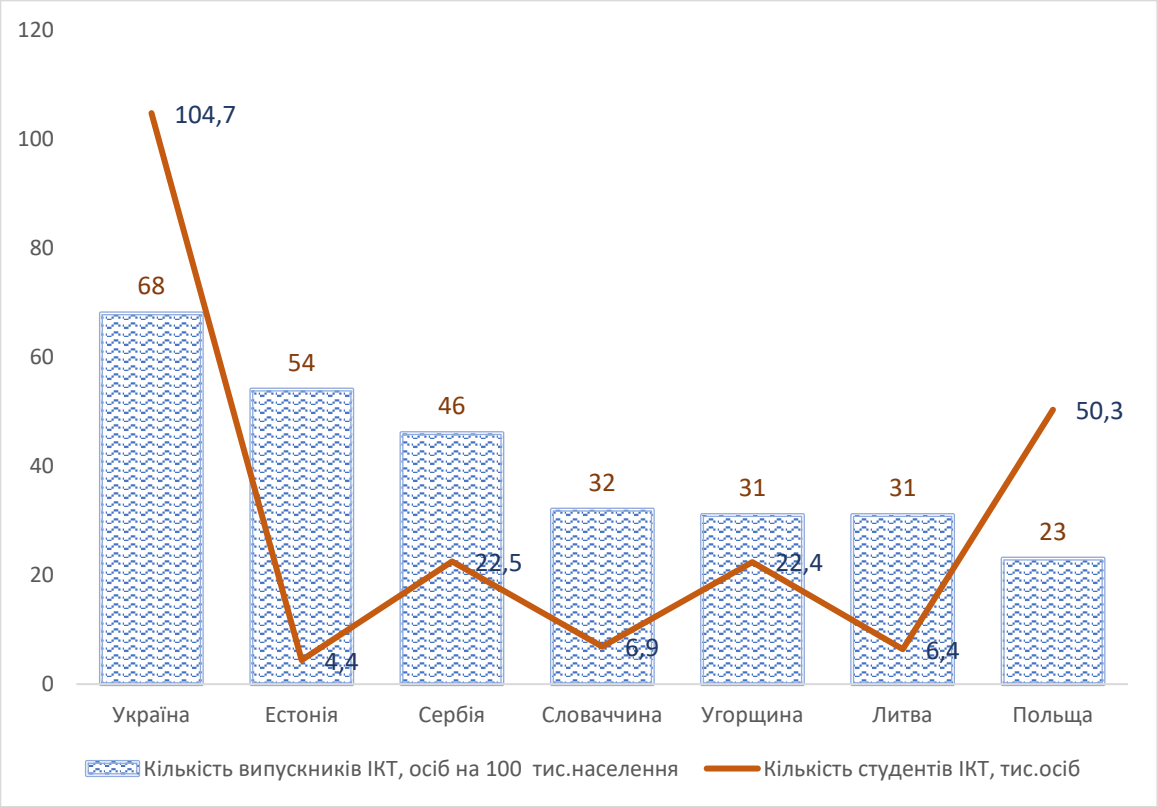


Рис. 3. Кількість студентів ІКТ та кількість випускників ІКТ (Держстат, 2023)

З урахуванням сучасних тенденцій глобалізації інформаційного простору, динамічної трансформації інформаційних ризиків, гібридних загроз, кібернетичних атак і нападів гостро

постає потреба забезпечення ефективності digital-маркетингу у системі публічного управління.

У сучасних умовах діджиталізації всіх сфер суспільної діяльності гостро постає потреба аналізу ефективності та захищеності інформаційної діяльності.

Саме цими питаннями опікується аналітика цифрового маркетингу, зокрема в системі публічного управління. Саме передбачувальна аналітика (прогностичний аналіз) сприяє виявленню потреб потенційних користувачів послуг.

А відтак, аналіз digital-маркетингу, який, зазвичай, поділяють на екзогенний та ендогенний, шляхом детального аналізу цілого спектру характеристик з урахуванням нюансів, формує, шляхом використання ресурсів digital-маркетингу, підґрунтя для розробки стратегій подальшого розвитку.

У digital-маркетингу існує безліч ресурсів, які в основному можна розділити на три групи: платні ресурси, власні ресурси, безоплатні комунікаційні канали (рис. 4).

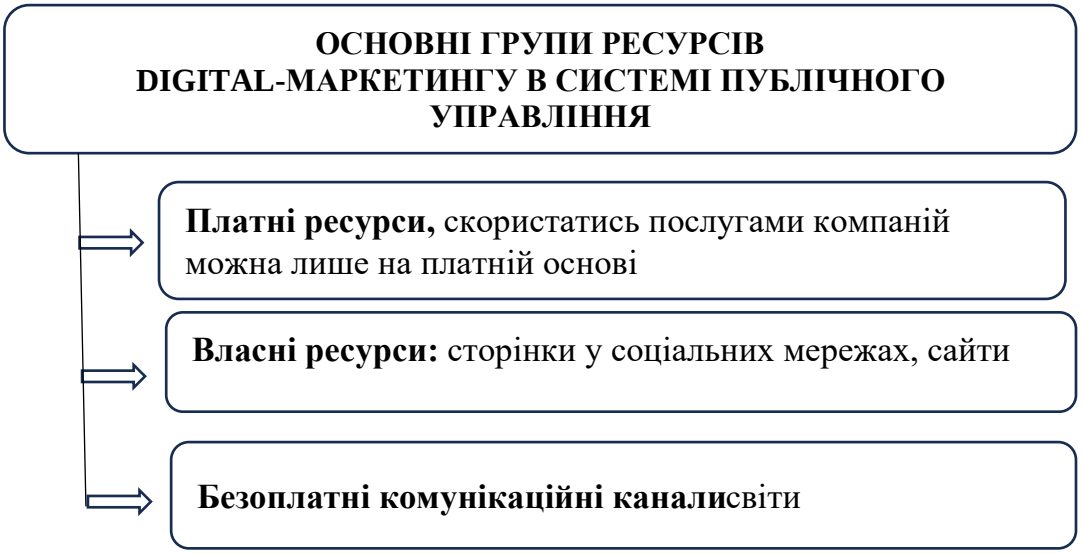


Рис. 4. Основні групи ресурсів digital-маркетингу в системі публічного управління.

Цифровий маркетинг в системі публічного управління передбачає використання різних числових каналів та технологій для просування товарів та послуг, серед яких платформи соціальних мереж, пошукові системи.

Digital-маркетинг у системі публічного управління, окрім використання традиційних каналів цифрового маркетингу (рис. 5), використовує й інструменти персоніфікації, чим підсилює вплив маркетингового впливу на цільову аудиторію.

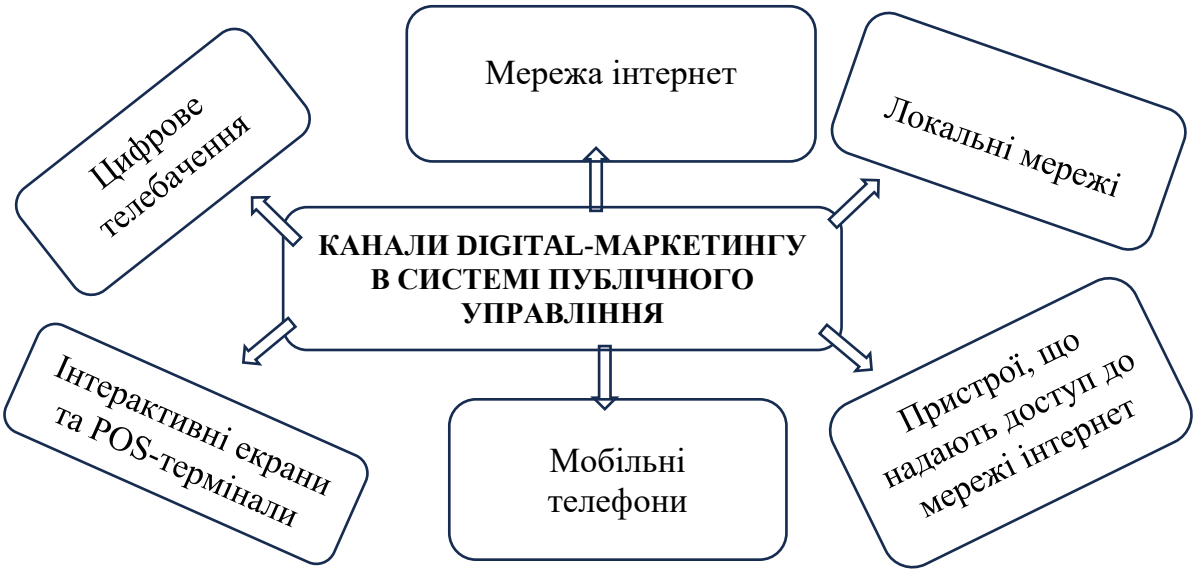


Рис. 5. Основні канали digital-маркетингу в системі публічного управління

Серед основних методів digital-маркетингу варто виокремити контекстну рекламу, мобільний маркетинг та ін. (рис. 6).

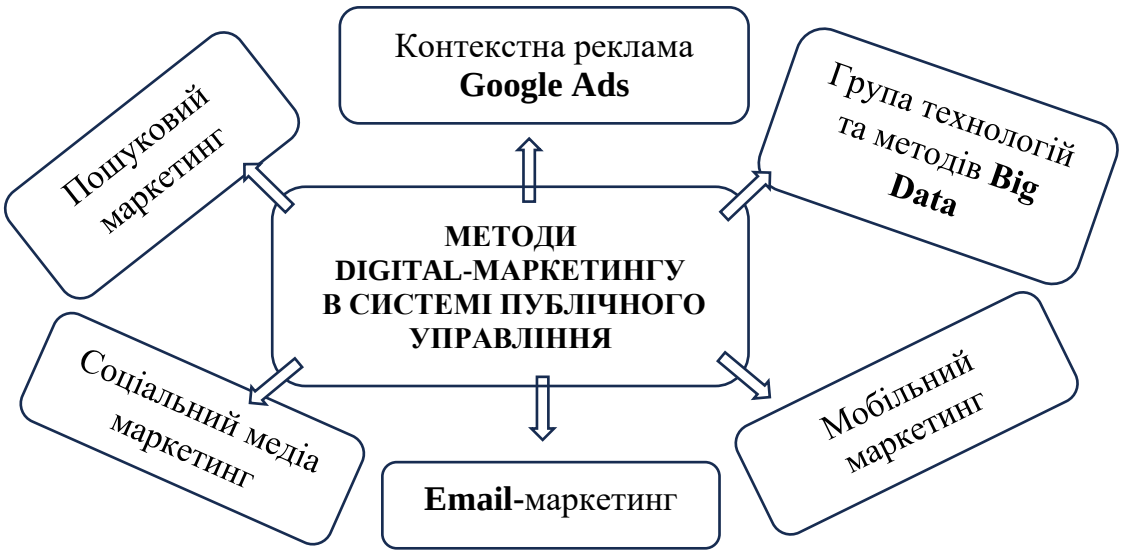


Рис. 6. Методи digital-маркетингу в системі публічного управління

Digital-маркетинг в системі публічного управління, базуючись на аналітиці даних про користувачів, аналізі їх уподобань та поведінкових трендах, проникає у традиційні види комунікацій з метою заволодіти увагою аудиторії та зосередити її у сфері актуальних дискусійних питань чи проблем.

Упровадження digital-маркетингу в систему публічного управління передбачає здійснення системного неперервного аналізу екзогенного та ендогенного середовищ, базується на аналітиці даних про користувачів, передбачає персоніфікацію, яка підсилює вплив маркетингових інструментів на цільову аудиторію *(Дяченко В., Дяченко Н., 2024)*. Ендогенна аналітика включає збір, аналіз та інтерпретацію даних, отриманих з різних джерел всередині державних органів, установ чи організацій. Отримана інформація стане підґрунтям для оцінки ефективності діяльності. Аналіз показників відвідування сайту державного органу, установи чи організації користувачами сприятиме розробці стратегії його удосконалення.

Одним з інтернет-ресурсів, які допомагають оперативно моніторити таку інформацію є, наприклад, зручний та багатофункціональний сервіс від компанії Google Google – Google Analytics за допомогою інструментів якого зручно здійснювати моніторинг статистики користувачів, кількості сеансів, нових користувачів, показник відмов, середню тривалість сеансу тощо.

Такий аналіз дозволяє відчути зацікавленість аудиторії, сприяє розумінню її потреб, а відтак, задає вектор коригування власних маркетингових стратегій.

У сучасних умовах становлення засад інформаційного суспільства digital-маркетинг є запорукою ефективності діяльності органів публічного управління.

Цифрові канали наділені гіпермедійною можливістю, забезпечуючи практично миттєве поширення інформації, вони є основним носієм комунікаційних повідомлень та ефективної взаємодії усіх стейкхолдерів.

Аудіовізуальні цифрові технології забезпечують можливість здійснення бажаного психологічного, емоційного та когнітивного впливу на цільову аудиторію без обмежень щодо геолокації комп’ютера, сприяють формуванню механізмів адаптивного управління в режимі реального часу.

Серед переваг digital-маркетингу в системі публічного управління варто виокремити оперативність, можливість розширення аудиторії як онлайн- так й офлайн-користувачів та динамічність процесів коригування управлінських рішень з урахуванням потреб як державних органів, установ чи організацій, так і користувачів.

Водночас, сучасний розвиток інформаційних технологій, сприяючи інтенсифікації процесів отримання, накопичення, обробки та зберігання інформації, обумовлює потребу забезпечення захисту інформації – приватної, комерційної, державної.

Адже, несанкціоноване використання інформації –стратегічного ресурсу підприємства, установи чи організації, може мати й дестабілізуючі наслідки (Дяченко В., Безсонова Д.,

Дяченко Н., 2023). А відтак, варто системно здійснювати моніторинг загроз (рис. 7), диверсифікувати ризики та вчасно нівелювати їх негативні наслідки.

Рис. 7. Основні загрози кібернетичної безпеки у сфері digital-маркетингу

Глобалізаційні трансформаційні процеси обумовлюють потребу в оперативному доступі до актуальної інформації. В умовах воєнного стану в Україні гостро постає потреба доступу до актуальної, правдивої, неупередженої інформації, отриманої з першоджерел. Саме застосування інструментів цифрового маркетингу в системі публічного управління сприяє підвищенню ефективності управлінської діяльності державного органу, установи чи організації. Водночас, варто, з урахуванням найбільш актуальних загроз, приділяти увагу захисту інформації (державної, приватної чи бізнес-інформації) від несанкціонованого доступу шляхом безпечного використання інформаційних систем, що сприятиме доступності до публічної інформації, збереженню її цілісності та, за потреби, конфіденційності.

У процесі упровадження digital-маркетингу в систему публічного управління необхідно дотримуватись заходів кібернетичної безпеки, зокрема шляхом упровадження SSL протоколів (англ. Secure Sockets Layer – рівень захищених сокетів), регулярно оновлювати системи та здійснювати резервне копіювання даних, що сприятиме нівелюванню вразливостей та захисту інформації від несанкціонованого доступу.

Водночас ІТ-бізнес, є одним з найбільш динамічних, і тому важливо, щоби всі відносини між його учасниками були належним чином врегульованими, зокрема

корпоративними та/чио акціонерними договорами. Основними учасниками ІТ-бізнесу є споживачі, особи, які створюють продукт інтелектуальної власності та безпосередньо акціонери (партнери) юридичної особи,яка надає такі послуги споживачам, тому питання чіткого врегулювання між партнерами компанії є дуже важливим.

Не достатній рівень врегулювання питання корпоративного договору на законодавчому рівні породжує потребу бізнес-партнерам врегульовувати свої відносини в інших юрисдикціях, саме тому, укладаючи корпоративний договір, сторони намагаються врегулювати різні питання щодо ведення бізнесута управління компанією, а саме: порядок виплати дивідендів, забо- рону продажу частки протягом певного періоду часу або обов'язок чи право продажу своєї частки при настанні певних обставин, механізм вирішення не узгоджених питань тощо. Саме тому питання щодо врегулювання спорів, які виникають в рамках корпоративного договору потребує удосконалення нормативно-правового забезпечення. Недосконаліть законодавства та відсутність належної судової практики призводить до того, що партнери вимушені створювати компанії в інших юрисдикціях, що негативно позначається на економіці України.

У сучасному демократичному суспільстві інформаційна сфера відіграє важливу роль у суспільному устрої та його прогресивному розвитку.

Інформаційна сфера є важливим чинником суспільно-державних зв'язків, проте вона не є автономною. Для сталого розвитку суспільства та держави важливо системно удосконалювати нормативно-правове регулювання ефективного функціонування інформаційної сфери. Базовим елементом інформаційної сфери є інформація.

Пріоритетом конституційних засад, які є невід'ємною складовою становлення суверенної України, щодо регулювання інформаційної сфери, є забезпечення прав і інтересів людини, суспільства та держави, щодо відкритості, доступу та захисту нформації.

Належне забезпечення захищеності інтересів людини, суспільства та держави в інформаційній сфері є важливою задачею, яка потребує додаткового аналізу теоретичних положень та конституційних засад забезпечення інформаційної безпеки України. Цей аналіз сприяє окресленню основних характеристик та особливостей інформаційної безпеки, а також обґрунтуванню напрямків розвитку конституційного регулювання в цій сфері.

В умовах становлення засад інформаційного суспільства, у якому діяльність людей ґрунтується на використанні послуг, що надають за допомогою інформаційних технологій і технологій зв'язку, державі належить провідна роль у координації діяльності різних його суб'єктів публічного простору

Інформаційне суспільство, як складова громадянського суспільства, що функціонує в

межах єдиного інформаційно-комунікаційного простору, у якому домінують нові технологічні засади, що передбачають масове використання перспективних інформаційних технологій, засобів комп'ютерної техніки, телекомунікацій, сприяє реалізації інформаційних прав і свобод людини, зокрема прав на безпечне вільне отримання, поширення та використання інформації.

Конституція України містить ряд положень, що безпосередньо спрямовані на регулювання інформаційної сфери суспільних відносин в Україні:

– стаття 34 визначає право на свободу думки і слова, а також право на інформацію;

– стаття 39 гарантує право на вільний доступ до інформації, у тому числі до державної інформації;

– статтею 17 передбачено формування інформаційної безпеки;

– стаття 50 гарантує право вільного доступу до екологічної інформації;

– стаття 57 Конституції України гарантує доступ до правової інформації *(Конституція України, 1996)*.

Ці положення відображають соціальну цінність інформації для людини, її право на отримання та поширення інформації.

Конституційні засади правового регулювання інформаційної сфери мають на меті формування інформаційної безпеки, гарантування права на інформацію, включаючи право на свободу думки і слова, а також забезпечення права доступу до інформації.

Упровадження інформаційно-комунікаційних та цифрових технологій в процеси публічного адміністрування

У сучасному глобалізованому світі інформація є одним з найцінніших ресурсів для всіх верств населення. Зростаючий попит на відкритість та доступність інформації – це характерна риса демократичного суспільства. Водночас зі збільшенням відкритості й прозорості зростають й потенційні загрози, пов'язані із діями кіберзлочинців, які можуть мати наміри щодо спричинення шкоди конфіденційній інформації, що актуалізує потребу гарантування балансу між вимогами до відкритості та доступності інформації даних, зокрема в органах державної влади та місцевого самоврядування. Забезпечення доступу кожного до інформації та забезпечення інформаційної безпеки України є основними напрямами державної інформаційної політики.

Громадяни мають право оперативного доступу до інформації щодо діяльності органів влади та мати безпосередню можливість щодо участі у прийнятті рішень. Забезпечення відкритості та прозорості інформації – це необхідна складова передумова демократичного світу, адже доступ громадян до інформації безпосередньо впливає на формування довіри до

органів державної влади та місцевого самоврядування. У свою чергу, підвищення соціальної активності громадян стимулює відповідальну роботу представниківорганів державної влади та місцевого самоврядування. Забезпечення максимального доступу до інформації в органах державної влади та місцевого самоврядування повинно поєднуватися з забезпеченням захисту інтересів національної безпеки України.

Інформатизація суспільства в усіх сферах публічних відносин динамічно впроваджується, тож питання безпечного публічного адміністрування обумовлює потребу системної модернізації механізмів захисту інформації публічної, підприємницької чи приватної. Це стосується й механізмів автоматизації судових процесів через всесвітню мережу інтернет та засобів мобільного зв'язку, що вже стали буденною справою, прикладом тому є запровадження веб порталу «Дія». А відтак, розвиток та впровадження публічного адміністрування питань безпеки в інтелектуальному вимірі є наразі актуальним та обов'язковим процесом. Незважаючи на те, що фахівці в IT сфері активно працюють над посиленням захисту застосунку, серед проблем додатку «Дія» варто виокремити: зникнення даних, несвоєчасне «підтягування» інформації, довга верифікація та некоректна робота застосунку. Командою Міністерства цифрової трансформації на платформі Bugcrowd за підтримки агентства з міжнародного розвитку США (USAID) проведено тестування на знаходження можливих помилок у «Дія» з призовим фондом в 1 млн грн. Слід зазначити, що у застосунку не виявили вразливостей, які б суттєво впливали на безпеку. Під час експерименту було знайдено два технічних баги найнижчого рівня, які одразу були виправлені.

У сфері впровадження публічного адміністрування становлення безпеки в інтелектуальному вимірі існують деякі проблеми, які безпосередньо стосуються недосконалості правового регулювання та невизначеності електронних баз даних. Водночас, незважаючи на вказані недоліки, в цій сфері є такі суттєві переваги, серед яких: доступність, зручність та ефективність доступу до електронних послуг громадян, що й актуалізує потребу вдосконалення нормативно-правової бази та безпекового середовища надання публічних адміністративних послуг. Інформаційна безпека, як стан захищеності особистості, суспільства та держави від ендогенних та екзогенних інформаційних загроз, при якому забезпечуються реалізація конституційних прав і свобод людини та громадянина, гідна якість та рівень життя громадян, суверенітет, територіальна цілісність та стійкий соціально-економічний розвиток, оборона та безпека держави *(Цимбал Б., 2023)* є набором інструментів та процедур, які захищають державну, підприємницьку чи приватну інформацію від неправомірного використання, несанкціонованого доступу, пошкодження чи знищення.

Термін «цифрова безпека» вживається у вітчизняній науці у зв'язку з дослідженням цифрових об'єктів та використовується для позначення різноманітних аспектів захищеності у цифровому середовищі. Цифрова безпека є станом захищеності від загроз, що виникають в умовах нового цифрового технологічного устрою, у тому числі викликаних використанням цифрових технологій у публічному управлінні, цифровізацією економіки, освіти, медицини та інших сфер освіти й приватного життя. Цифрові технології, як технології передачі інформації, та розвиток штучного інтелекту, цифрової електроніки, біометрії, стільникового зв'язку, телемедицини, смартміст, навігації, робототехніки .актуалізують потребу забезпечення ефективності кібернетичної безпеки

В умовах поширеної цифровізації актуалізується потреба подальшого розвитку безпеки в державному управлінні на інтелектуальному рівні, зокрема через доктринально-інформаційне наповнення, механізми сучасного державного управління та реалізацію окремих принципів цифрової безпеки. В умовах цифровізації публічного управління, економіка таправо повинні координувати діяльність органів державної влади та місцевого самоврядування, приватних інституцій, суспільства, суб'єктів цифрового бізнесу та креативного інформаційного середовища.

Враховуючи процеси динамічного розвитку інформаційних технологій у публічному адмініструванні, питанням становлення безпеки в інтелектуальному вимірі доцільно приділяти більше уваги.

З метою формування ефективності безпеки інформації державної, підприємницької чи приватної необхідно:

– розробити та впровадити механізми захисту конфіденційної інформації включаючи виявлення фішингу, застосування складних та двоетапних перевірок входів в систему, застосування криптографічного захисту інформації, шифрування даних;

– створити інструкцію щодо запобігання від внутрішніх ендогенних та екзогенних загроз цілісності інформації, застосування самостійного та автоматичного виявлення інцидентів, які вказують на підозрілу активність чи потенційну можливість загрози хакерської атаки;

– залучати інноваційні технології та здійснювати оновлення застарілих інформаційно-телекомунікаційних технологій;

– формувати безпечні умови зберігання конфіденційної інформації від всіх видів загроз за допомогою сучасних систем захисту;

– проводити аудити безпеки та застосування самоперевірок справності системи для визначення потенційних вразливостей та слабкостей системи.

Ці підходи та комплекси можуть взаємодіяти та доповнювати один одного, створюючи систему, яка забезпечить ефективний та інноваційний доступ до інформації в органах державної влади та місцевого самоврядування з урахуванням положень безпеки. Упродовж 2021 року IT галузь демонструвала сталу позитивну динаміку експорту послуг, за результатами року сума експорту становила 6,5 млрд дол., що на 36% більше, ніж у 2020 році (5 млрд дол.). У зв'язку з введенням у лютому 2022 року воєнного стану загальний експорт послуг у березні місяці скоротився на 41 %, при цьому становив 52 % у складі загального експорту послуг України. За підсумками 2022 року IT-сектор, єдина галузь, що зорієнтована на експорт, продовжила стрімке зростання попри падіння економіки на тлі воєнного стану *(Веселовський С., 2022)*. Такі ж тенденції й у 2023 році, зокрема IT-експорт послуг у травні 2023 року зріс на 9,5 % у порівнянні з попереднім місяцем *(Пилипів І., 2023)*, обумовлюючи потребу модернізації правових інструментів публічного адміністрування експорту та імпорту товарів та послуг, зокрема військового та подвійного призначення. Правове врегулювання передбачає врегулювання суспільно-економічних відносин з метою отримання соціального корисного результату, що здійснюється на основі принципів права. Досягнення запрограмованих позитивних результатів публічного адміністрування суб'єктами владних повноважень можливе лише шляхом застосування правових засобів – інструментів публічного адміністрування, зокрема у сфері формування національної безпеки, вагомою складовою якої є правове врегулювання питань забезпечення експорту та імпорту товарів та послуг військово та подвійного у тому числі. В умовах правового режиму воєнного стану в Україні, оголошеного 24 лютого 2022 року питання правового регулювання експорту та імпорту товарів та послуг військового та подвійного набуло пріоритетного значення, у світлі формування засад національної безпеки, зокрема при здійсненні імпорту зброї та товарів військового призначення для потреб Збройних сил та сил оборони України.

У теорії адміністративного права правові аспе кти інструментів публічного адміністрування характеризуються певними ознаками, зокрема вони є екзогенним проявом форми публічної діяльності адміністративного органу, які віддзеркалюють правову динаміку процесів публічного адміністрування. Системне впровадження інноваційних безпекових підходів, удосконалення нормативно-правової бази, підвищення рівня свідомостігромадян є запорукою успіху на шляху до формування засад безпечного доступу до інформації державної, підприємницької чи приватної, адже вони є комплексом адміністративно-правових заходів, які безпосередньо використовують адміністративні органи з метою формування засад забезпечення прав, свобод і законних інтересів приватних осіб, бізнесу та публічного інтересу держави й суспільства, оскільки, інструмент публічного адміністрування – це екзогенний

вираз однорідних за своїм характером і правовою природою груп публічних дій адміністративних органів, реалізованих у межах відповідності визначеної законом компетенції з метою досягнення бажаного публічного інтересу. Базовим правотворчим інструментом публічного адміністрування є прийняття Верховною Радою України законів та їх поточне редагування у відповідності до вимог часу.

В умовах сьогодення гостро постає питання захисту персональних даних.

Варто врахувати, що особливого захисту своїх персональних даних через призму публічного адміністрування потребують ті, хтосвоїми зусиллями наближає нас до перемоги.

Висновок. Організація сучасного освітнього процесу у закладах вищої освіти повинна сприяти задоволенню потреби здобувачів вищої освіти у творчій самореалізації, та інтелектуальному самовдосконаленню шляхом безперервного розвитку особистості. З урахуванням сучасних тенденцій глобалізації інформаційного простору, динамічній трансформації інформаційних ризиків та загроз, кібернетичних атак і нападів необхідно забезпечити здобувачам вищої освіти високий рівень знань, умінь та практичних навичок у сфері інформаційно-телекомунікаційних технологій.

У зв'язку з інтенсивним розширенням сфери використання дронів у приватному використанні, сільському господарстві та у Збройних Силах України необхідно розширити перелік освітніх компонентів для здобувачів вищої освіти галузі інформаційні технології, зокрема збільшити обсяги на викладання:

– апаратно-програмного забезпечення комп'ютерних систем координації дронами;

– оператор дрону (безпілотного літального апарату).

Упровадження хмарних технологій у навчальний процес ефективно здійснюється упродовж останніх років. Закладам вищої освіти доцільно розгорнути кіберполігони, адже, використання кіберполігону сприяє формуванню у здобувачів вищої освіти компетентностей, що сприятимуть їх конкурентоспроможності на ринку праці.

З урахуванням сучасних тенденцій, майбутніх потреб на ринку праці, зокрема й при повоєнній відбудові, закладам вищої освіти необхідно до викладацької діяльності залучати висококваліфікованих фахівців-практиків для забезпечення рівня викладання інформаційних технологій відповідно до сучасних стандартів, вимог професійної діяльності, потреб формування засад інформаційної, національної безпеки, потреб суспільства та пріоритетів повоєнної відбудови.

Конституційні засади формування безпеки інформаційної сфери є невід'ємною частиною Конституції України, яка визначає основні принципи та правові норми, спрямовані на захист і розвиток інформаційного простору. Ці положення також виступають правовою основою для формування національного законодавства щодо інформаційної безпеки та покликані гарантувати

відповідність правового регулювання питань інформаційної безпеки в Україні міжнародним стандартам та вимогам світового інформаційного суспільства, зокрема у питаннях адміністративно-правового захисту персональних даних.

References:

Spirin O., Vakaliuk T. (2019) Formation of information and communication competence of bachelors of informatics regarding the use of a cloud-oriented educational environment. *Information Technologies and Learning Tools*, vol.72, no.4, 2019. https://doi.org/10.33407/itlt.v72i4.3262.

Kapiton A. (2023) Information and computing competence of future specialists in information technologies. *Information Technologies and Learning Tools*, vol.93, no.1, 2023. doi: https://doi.org/10.33407/itlt.v95i3.5195.

Abysova M, Kravchuk M, Hurniak O. (2023) Digitalization in university education: didactic aspects. *Information Technologies and Learning Tools*, vol.93, no.1, 2023. https://doi.org/10.33407/itlt.v93i1.5097.

Pokhre S, Chhetri R, Literature A. (2021) Review on Impact of COVID-19 Pandemic on Teaching and Learning. *Higher Education for the Future*, vol.8, no.1, 2021. https://doi.org/10.1177/2347631120983481.

Bamforth S., Perkin G., Flint J. (2019) Understanding the student perspective of Microsoft OneNote as a learning resource in higher education. *ICERI2019 Proceedings,* 2019.

Lavi R., Tal M., Dori Y. (2021) Perceptions of STEM alumni and students on developing 21st century skills through methods of teaching and learning. *Studies in Educational Evaluation*, vol.70, 2021. https://doi.org/10.1016/j.stueduc.2021.101002.

Polyviou A., Venters W., Pouloud N. Distant but close: Locational, relational and temporal proximity in cloud computing adoption. *Journal of Information Technology*, vol.38, 2023. doi: https://doi.org/10.1177/02683962231186161.

Gautam A, Bansal A. Effect of Features Extraction Techniques on Cyberstalking Detection Using Machine Learning Framework. *Journal of Advances in Information Technology*, vol.13, 2022. doi: https://doi.org/10.12720/jait.13.5.486-502.

Novachenko T., Bielska T., Afonin E., Lashkina M., Kozhemiakina O., Diachenko N. (2020) Use of Information Technology to Increase Economic Efficiency and Credibility in Public Administration in the Context of Digitization. *International Journal of Economics and Business Administration*, vol.VIII, no.1, 2020. URL:https://ijeba.com/journal/431.

EU Data Portal (2022) Open Data Maturity 2022. URL: https://data.europa.eu/en/publications/open-data-maturity/2022.

WIPO. (2022) Global Innovation Index 2022". URL: https://www.wipo.int/global_innovation_index/en/2022/.

About information protection in automated systems (1994). Law of Ukraine № 80/94-BP. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

Tarasovskyi Yu. (2022) Up to 57000 IT specialists left Ukraine, about 7000 joined the Armed Forces - research.URL: https://forbes.ua/news/do-57-000-it-spetsialistiv-viikhali-z-ukraini-blizko-7000-vstupili-v-zsu-doslidzhennya-01082022-7461.

Work.ua. (2024) URL: https://www.work.ua/jobs-kyiv-it/.

Rubryka (2023) In 2022, the Ukrainian market of spraying drones became No. 1 in Europe. URL: https://rubryka.com/2023/02/26/u-2022-rotsi-ukrayinskyj-rynok-droniv-obpryskuvachiv-stav-1-u-yevropi/.

Militarnyi (2022). The Ukrainian military will receive D-80 Discovery and E-300 Enterprise UAVs. URL: https://mil.in.ua/uk/news/vijskovi-ukrayiny-otrymayut-bpla-d-80-discovery-ta-e-300-enterprise/.

Production Ready (2023) Top 5 technological trends of 2023. URL: https://production-ready.dev/2023/01/5-it-trendiv-2023/.

Diachenko V., Diachenko N., Golubkov I. (2024) Features of ensuring intellectual property rights in the field of digital technologies. *Global science: prospects and innovations. Proceedings of the 7th International scientific and practical conference.* Cognum Publishing House. Liverpool, United Kingdom. 2024.

Diachenko V., Diachenko N (2024) Peculiarities of the state policy regarding the provision of intellectual property rights in the field of digital technologies. *Public administration: improvement and development.* no.2, 2024. https://doi.org/10.32702/2307-2156.2024.2.17.
Online Institute Creative&Tech PTJCTR (2023). URL: https://prjctr.com/.
Bondarenko O. (2023) Qualification mismatch of employees of EU countries in the context of mastering digital skills. *Information Technologies and Learning Tools*, vol.95, no.3, 2023. https://doi.org/10.33407/itlt.v95i3.5195.
Information telethon "Edyni Novyny" (#UArazom) - 100 days on the air (2022). URL: https://www.kmu.gov.ua/news/informacijnij-telemarafon-yedini-novini-uarazom-100-dniv-v-efiri.
Global Digital Marketing Market Report and Forecast 2023-2028 (2023). URL: https://www.researchandmarkets.com/reports/5775236/global-digital-marketing-market-report-forecast**.**
Global Innovation Index(2022). URL: https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2022-en-main-report-global-innovation-index-2022-15th-edition.pdf.
State Statistics Service of Ukraine (2023). URL: https://www.ukrstat.gov.ua/.
Diachenko V., Diachenko N.Публічний digital-маркетинг як елемент державної інформаційної політики. Наукові перспективи. 2024. № 2 (44).С.245-254. https://doi.org/10.52058/2708-7530-2024-2(44)-245-254.
Diachenko V., Bezsonova D., Diachenko N. (2023) Formation of information security in conditions of martial law. *Modernization of the economy: current realities, predictive scenarios and prospects for development: materials of the International science and practice conf.* (April 27-28, 2023, Kherson, Khmelnytskyi), 2023.
Constitution of the Ukraine (1996). URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
Tsymbal B. (2023) The mechanism of public management of personal safety: a qualitatively new dimension in the system of digital technologies and innovations. https://doi.org/10.32843/ pma2663-5240-2022.30.15
Veselovskyi C. (2023) IT is the only industry that will grow in 2022: why rejoice too early. URL: https://rubryka.com/blog/it-industry-grew-in-2022/.
Pylypiv I.(2023) In May, the export of IT services from Ukraine increased by 9.5% compared to last month. URL: https://www.epravda.com.ua/news/2023/07/1/701797/.

DOI 10.5281/zenodo.10822042
UDC 004.8:327(100)-049.5

CHAPTER 19.
ARTIFICIAL INTELLIGENCE IN INTERNATIONAL SECURITY SYSTEMS: EFFICIENCY IN THE ERA OF SMART STATE EMERGENCE

Iaroslav DOROHYI
DSc., Professor, Professor of Department Applied Mathematics and Informatics,
Donetsk National Technical University,
yaroslav.dorohyi@donntu.edu.ua,
https://orcid.org/0000-0003-3848-9852

Olena DOROHA-IVANIUK
Teacher of the highest category in informatics, Pology Lyceum of Kovalivsk Village Council,
Belotserkiv District, Kyiv Region
dioo@polohivskyinvk.net
https://orcid.org/0000-0003-3640-6312

Iryna BERDYCHENKO
PhD in Law, Associate Professor of Department of Criminal Law and Procedure, Kyiv University of Law of the National Academy of Sciences of Ukraine,
irinaberdychenko@gmail.com,
https://orcid.org/0000-0002-6670-433X

Abstract. This article explores the use of AI in international security systems and its role in the effective functioning of modern "smart states." The main principles and possibilities of using AI for detecting, predicting, and countering cyber threats, monitoring and optimizing border control processes, forecasting and early warning of conflicts, optimizing humanitarian aid, and crisis response are considered. Various technical innovations and their potential in addressing security issues are discussed. This article aims to analyze in detail the impact of AI on enhancing the efficiency and security of international relations, especially in the context of the emergence of the "smart state" concept. The advantages and possible risks of AI application in the security sphere are examined, and prospects for further development in this research direction are identified.

The article also highlights the legal aspect of AI implementation and regulatory framework in Ukraine. The main problems requiring legislative resolution in the field of AI technology usage in various spheres of society's life are identified. Attention is focused on the necessity of legal regulation for protecting democratic human rights in AI technology access. Various options for legal regulation of AI usage are proposed. Psychological aspects of AI-human interaction are outlined. Understanding the principles and strategic decisions for AI implementation in a smart state are proposed.

Key words. AI, artificial intelligence, smart state, international security systems, law aspects of AI, smart state emergence.

Introduction. Artificial intelligence (AI) in all spheres of societal life is a prospect within the next 5-10 years. This is a global trend. In the field of international security, the use of artificial intelligence (AI) is an important component of security strategies, particularly in the context of shaping the concept of a "smart state." Today, AI includes machine learning, computer vision, deep learning, and natural language processing (NLP).

AI is becoming one of the main tools for building and developing smart states, and accordingly, achieving strategic goals in ensuring welfare, comfort, and quality of life for the population, building a safe environment, and developing the economy, where key factors of production will be AI technologies, the emergence of new industries, improving the quality of government services, and saving human and material resources. The trend towards AI displacing humans from their usual processes—production, service sectors, entertainment, trade, education, and even medicine—is not a fantasy but an existing reality with a tendency to expand.

The task of a smart state is to lead these processes and ensure their effective coordination. Key initiatives regarding artificial intelligence should be the formation of priorities in motivating the use of AI technology instead of traditional tools by consumers, including both businesses and ordinary citizens, understanding the benefits of this, fostering national AI projects, and finding relevant models of public-private partnerships for their implementation.

Today, there are administrative, organizational, legal, and ethical challenges associated with the widespread implementation of AI that require the development of strategies and planning to overcome them. The current task is to understand and prepare appropriate initiatives, both managerial, technological, and legislative, to stimulate the transition from traditional ways of organizing society and state functioning to innovative ones that involve extensive use of AI.

Accurate and timely data to support decision-making and development planning in various sectors of societal life, access to affordable high-quality AI solutions for the population, cooperation and knowledge exchange, progress, and innovative solutions aimed at improving the quality of life

of citizens—all these are endless possibilities that will ensure further development of artificial intelligence.

The future belongs to states and societies that overcome the barrier between people and AI technologies and create conditions for the effective development of the AI ecosystem, significantly enhancing their capabilities to be efficient, competitive, and safe, providing their citizens with new opportunities for development and self-realization.

I. Artificial Intelligence in International Security Systems

I.1. Management Aspects of AI Usage. AI is becoming increasingly prevalent in many spheres of life, and its use brings along a range of management aspects that require careful study. Here are some of them:

1. *Ethics and Responsibility*. The use of AI can have ethical implications such as bias, discrimination, and privacy violations. It is important to establish clear ethical principles and rules to regulate AI usage and ensure its responsible application.

It is necessary to clearly define who is responsible for the actions and decisions made by AI systems, including at the legislative level.

2. *Job Transformation*. AI can automate many tasks previously performed by humans, potentially leading to job losses. It is important to develop retraining and upskilling programs to help people adapt to changes in the labor market.

3. *Transparency and Explainability*. AI systems can be complex and opaque, which can make it difficult to control their operation and explain their decisions. Ensuring transparency in the operation of AI systems is important so that people can understand how decisions are made.

4. *Cybersecurity*. AI systems can be vulnerable to cyberattacks, leading to data theft, system malfunctions, and other problems. It is important to take measures to protect AI systems from cyber threats. One possible solution to this problem is to develop cybersecurity standards for AI systems.

5. *Regulation*. The use of AI may require new regulations to ensure its safe and ethical use. It is important to develop clear and flexible regulations that keep pace with the development of AI technologies.

6. *Economic Implications*. The use of AI can have significant positive and negative impacts on the economy. It is important to assess the potential economic implications of AI usage and develop policies that stimulate its positive impact. Investing in AI research and development is important to stimulate economic growth.

7. *Social Implications*. The use of AI can have significant positive and negative impacts on society. It is important to assess the potential social implications of AI usage and develop policies that stimulate its positive impact.

8. *International Cooperation*. Since AI is a global technology, it is important to establish international cooperation to ensure its safe, ethical, and responsible use. International cooperation aimed at developing common standards for ethics, responsibility, transparency, cybersecurity, and regulation of AI is advisable.

The use of AI can bring many benefits, but it also carries a number of risks. It is important to carefully study all the management aspects of AI usage to minimize risks and maximize benefits.

In the context of the security component, the management aspects of AI usage in international security systems include a wide range of issues related to management, strategic planning, and the effectiveness of AI usage for achieving security goals. Among the issues that AI can help address are:

- Strategic planning;
- Resource management;
- Process management;
- Ethical aspects.

The use of AI in international security systems opens up a wide range of opportunities to enhance efficiency and promptness in decision-making, threat monitoring, and analysis. Among the main directions of usage, the following can be named:

- *Forecasting and early warning of conflicts*. Artificial intelligence can analyze large volumes of data from various sources, including social media, news, diplomatic reports, and others, to identify early signs of conflicts or international tensions. AI-based analytical models can help identify key factors contributing to conflicts and develop recommendations for their avoidance or mitigation.

- *Monitoring and responding to cyber threats*. Artificial intelligence can be used for automated detection and analysis of cyber threats, including hacker attacks, malware, and cyber espionage. AI-based systems can detect anomalies in network traffic, analyze suspicious activity, and provide recommendations for protection and response to threats.

- *Optimization of humanitarian aid and crisis response*. Artificial intelligence can help optimize the distribution of humanitarian aid and response to crisis situations by analyzing geographic data, demographic characteristics, and other factors. AI algorithms can quickly and accurately assess the needs of populations in different regions and develop response strategies for international humanitarian organizations.

- *Monitoring and optimization of border control processes*. Monitoring and optimization of border control processes are important aspects of ensuring international security, especially in the face of increasing international mobility and threats of terrorism and illegal

migration. The use of AI can significantly facilitate these processes by providing fast and efficient border control. For example, AI can be used for monitoring border areas, analyzing individual behavior, recognizing and analyzing vehicles, optimizing flows, analyzing and forecasting risks.

– *Peacekeeping operations*. Peacekeeping operations are a key element of international security systems aimed at ensuring peace, stability, and security in conflict or post-conflict regions. The use of AI can play an important role in supporting and optimizing such operations. For example, AI can be used to analyze conflict situations, support decision-making, communication, and coordination processes, monitor compliance with international law, and so on.

– *Analysis of international treaties and political decisions*. Artificial intelligence can be used to analyze texts of international treaties, declarations, and political statements to identify trends, trends, and possible collisions in international relations. AI-based analytical systems can help diplomats and political analysts understand the consequences of decisions made and predict possible reactions of other countries.

I.2. Technical Innovations and Their Potential

I.2.1 Forecasting and Early Conflict Prevention. Forecasting and early conflict prevention are crucial aspects of ensuring international security. The use of artificial intelligence in this field can assist in timely identifying potential conflict situations and taking necessary measures to prevent them. Here are some methods that can be utilized for this purpose:

1. *Data and relationship analysis*: Employing machine learning algorithms to analyze large volumes of data from various sources such as news articles, social media, observer reports, etc. Identifying key patterns and relationships among different societal groups, political leaders, regions, and other factors that may indicate potential conflict situations.

2. *Monitoring social media and open sources*: Automatically tracking and analyzing messages on social media where warnings about potential conflicts or interethnic tensions may arise. Monitoring news sources and open media outlets to detect alarming signals and address hotspots.

3. *Conflict forecasting using machine learning models*: Developing predictive models based on historical conflict data to forecast potential conflict situations in the future. Utilizing forecasting algorithms to assess risks and identify hotspots where the likelihood of conflict is highest.

4. *Analysis of population dynamics and ethnic groups*: Using geographic information systems (GIS) and health data to analyze population dynamics, migration, and the distribution of ethnic groups, which may indicate potential conflict points. Modeling demographic and ethnic processes to forecast potential conflicts arising from the clash of interests among different groups.

A notable example of such an AI-based system is the Violence Early-Warning System (VIEWS) - an award-winning conflict prediction system that generates monthly forecasts of violent

conflicts worldwide for three years ahead. This system is supported by iterative research and development conducted by the VIEWS consortium *(Predicting conflict and humanitarian impacts. Available: http://surl.li/qljwd).*

I.2.2 Optimization of humanitarian aid and crisis response. Optimization of humanitarian aid and crisis response is a crucial aspect of ensuring international security, especially in the face of global crises and conflicts. The use of AI in this field can significantly enhance the efficiency and timeliness of humanitarian efforts. Some directions for optimizing humanitarian aid and crisis response using AI include the following:

1. *Crisis prediction*: Utilizing machine learning algorithms to analyze large volumes of data from various sources, including social media, observer reports, satellite imagery, and others, to identify early signs of crisis situations. Developing predictive models based on historical data to forecast potential crises and natural disasters.

2. *Resource management*: Employing analytics to determine the optimal distribution of humanitarian resources in crisis zones based on population needs, geographical location, and other factors. Establishing inventory monitoring systems and automatic alerts for replenishing supplies when a certain level of utilization is reached.

3. *Rapid response to emergencies*: Using AI systems to respond to automatic signals of emergency situations and activate necessary aid measures. Developing communication and coordination systems among humanitarian organizations, governmental structures, and other stakeholders for swift information exchange and action coordination.

4. *Impact analysis of humanitarian interventions*: Utilizing algorithms to analyze the effectiveness of humanitarian actions and identify the most efficient aid delivery strategies. AI can also assist in forecasting the consequences of humanitarian actions and developing strategies for recovery and rehabilitation after crisis situations.

Overall, the use of artificial intelligence can significantly improve the efficiency and effectiveness of humanitarian efforts and crisis response, allowing for faster and more efficient assistance to those in need *(Walter J., Gutjahr P., Nolz P., 2016).*

I.2.3 Monitoring and optimization of border control processes. Monitoring and optimization of border control processes are crucial aspects of ensuring international security, especially amidst increasing international movements and threats of terrorism and illegal migration. The utilization of artificial intelligence (AI) can significantly streamline these processes, providing swift and effective border control. Let's delve into this aspect in more detail:

1. *Monitoring border areas*: AI can analyze data from sensors, including radars, thermal cameras, and other sensors, as well as video recordings from surveillance cameras, to detect illegal border crossings and other violations.

2. *Behavioral analysis of individuals*: AI can utilize biometric data such as facial recognition, fingerprints, and iris recognition to identify individuals at the border and detect suspicious or dangerous persons. AI can analyze people's behavior at the border, identifying suspicious or abnormal actions such as nervousness, stress, or unusual movements that may indicate potential threats.

3. *Vehicle recognition and analysis*: AI can use vehicle license plate recognition technologies to identify suspicious or stolen vehicles at the border. AI can analyze data on crossing cargoes to detect dangerous materials, contraband, or other violations.

4. *Flow optimization*: AI can analyze data on people and vehicle flows, helping to predict border congestion and optimize resource allocation to ensure effective control. AI can automate certain border control processes, such as preliminary document checks or person identification, reducing wait times and increasing control efficiency.

5. *Risk analysis and prediction*: AI can use data on past events and other information sources to model potential threats and risks at the border, helping to ensure timely responses to potential threats.

The use of artificial intelligence for monitoring and optimizing border control processes can significantly improve the efficiency and safety of international security systems, ensuring effective control over the flow of people and goods at the border. Research is being conducted in this direction *(Tazrout Z. Available: http://surl.li/qlkhf),* transforming into technological solutions. For example, NurjanaTech's solution for border control takes a comprehensive approach to detecting and responding to threats among pedestrians, pack animals, vehicles, or vessels near the country's land and sea borders. These solutions employ a modular approach aimed at ensuring full integration between existing installations and new technologies *(Detecting, identifying, and reacting to threats in real-time. Available: http://surl.li/qlkio)* with capabilities to integrate radars, electro-optical systems, and other sensor data for real-time target detection, identification, and tracking, including artificial intelligence.

I.2.4 Peacekeeping operations. Peacekeeping operations are a key element of international security systems aimed at ensuring peace, stability, and security in conflict or post-conflict regions. The use of artificial intelligence (AI) can play an important role in supporting and optimizing such operations. Let's consider some aspects of using AI in peacekeeping operations:

1. *Analysis of conflict situations*: AI can quickly analyze large amounts of data from various sources, such as social media, observer reports, satellite imagery, etc., to provide an objective picture

of the conflict situation. AI can use machine learning algorithms to forecast potential risks and conflict situations based on the analysis of past events and other factors.

2. *Decision support*: AI can provide analytical support for assessing the situation and developing peacekeeping operation strategies based on objective data and risk analysis. AI can create computer models of situations and simulate various action strategies, assisting peacekeeping teams in making the most effective decisions.

3. *Communication and coordination*: AI can provide advanced information management systems to help coordinate actions between peacekeeping forces and other operation participants. The use of automated communication systems enables efficient communication between different elements of the peacekeeping operation, enhancing its coordination and effectiveness.

4. *Monitoring compliance with international law*: AI can be used to monitor compliance with international law in conflict zones, detect violations, and take appropriate actions. AI helps collect, analyze, and store data on violations of international law, creating an objective evidence base for further use in legal proceedings or other international actions.

The overall goal of using artificial intelligence in peacekeeping operations is to enhance their effectiveness and safety, improve understanding of the situation in conflict areas, and develop action strategies aimed at ensuring peace and stability.

A detailed description of the use of innovative technologies, including within NATO, is provided in *(New Technologies and the Protection of Civilians in UN Peace. Available: http://surl.li/qlklu).*

I.3. Legal Aspects of AI Implementation. The topic of regulating artificial intelligence is relevant today, and discussions on various levels are ongoing. The issue is global, affecting practically every country or region. Integrated efforts to regulate AI in the African continent are outlined in the "Digital Transformation Strategy for Africa (2020-2030)," approved by the relevant ministers of the African Union governments.

In the Asian region, the result of cooperation is the "Digital Master Plan" of the Association of Southeast Asian Nations, which defines the priorities for digital development in the region, including those related to AI, by 2025. Meanwhile, countries in South and Latin America are focused on developing national government approaches to regulating AI development, and supranational forms of interaction are not yet represented.

United Kingdom: Foundational standards for government regulation of AI-related processes are laid out in the National AI Strategy, prepared by the government of the United Kingdom and published on September 22, 2021, and the coordinating document "Creating an Innovative Approach

to AI Regulation," presented by the government on July 18, 2022. Among other things, they establish guidelines for shaping approaches to AI management.

Canada: Canada's government approach to AI aims to prepare future professionals in the AI field, support key innovation centers and research, and position the country as a leader in economic, ethical, political, and legal aspects of AI implementation. Canada was the first country in the world to create a National AI Strategy (the Pan-Canadian AI Strategy) at the government level, publishing it in 2017. To develop the provisions of the Pan-Canadian AI Strategy in 2019, the Government of Canada established the Advisory Council on AI.

To introduce new rules for responsible AI development and deployment, the Canadian government has introduced a comprehensive federal bill, C-27, "On the Implementation of the Digital Charter 2022," to Parliament, one of the legislative initiatives of which is the bill "On Artificial Intelligence and Data" (AIDA).

United Arab Emirates (UAE): According to the Networking Readiness technological index, published annually by the World Economic Forum, the UAE entered the top thirty most advanced countries in terms of information technology in its region as early as 2018. Such achievements are primarily explained by the state policy vector aimed at developing high digital technologies and implementing innovations, among which AI technologies play a crucial role.

United States of America (USA): The scale of involvement of intellectual resources concentrated in universities and research hubs in the USA, exemplified by Silicon Valley, ensures the country's leadership in creating AI technologies. Legislative regulation of AI technology usage at the federal level includes a series of systemic federal laws that regulate the formation of specialized institutions *(Holos Ukrainy vid 08.08.2023 r. Available: http://surl.li/qlkpe).*

In the EU, the formation of a regulatory framework for regulating AI technologies is taking place simultaneously at both the European governance level and in member states. The European Commission is currently responsible for developing policy in this area. At its initiative, the European AI Alliance has been established, which encompasses over six thousand stakeholders and serves as a platform for public discussions. In the near future, the creation of an independent body, the European Artificial Intelligence Board, is planned.

The Artificial Intelligence Act *(Artificial Intelligence Act. Brussels, 2021)* is a draft law of the European Union aimed at creating a safe environment for the use and development of AI. On December 9, 2023, the European Parliament reached a preliminary agreement with the Council on the AI law. The agreed text must be formally adopted by both the Parliament and the Council to become EU law.

The AI Act consists of 12 chapters, each regulating a separate area of application and development of artificial intelligence. This legislative proposal has an extraterritorial character. The main provisions of this legislative act include, among other things:

– defining the risk levels of AI systems;

– introducing mandatory certification for certain AI systems, such as biometric identification systems, critical infrastructure systems, educational or professional assessment systems;

– establishing requirements for certain AI systems regarding the necessity of informing users that they are interacting with an AI system rather than a human;

– setting transparency rules for AI systems intended to interact with individuals, emotional recognition systems, and AI systems used for creating or processing images, audio, or video content;

– prohibiting the use of certain AI methods.

The AI Act classifies AI programs by risk level and regulates them accordingly. It is based on a risk-based approach that classifies AI systems into five categories, as specified on the European Commission's website: prohibited AI systems; high-risk AI systems; limited-risk AI systems; low-risk or non-risky AI systems.

High-risk AI systems include those that have a significant impact on users' rights, health, or safety. These AI systems must comply with a list of mandatory requirements and undergo conformity assessment procedures before being placed on the EU market. Suppliers and users of these systems have clear safety obligations. Systems in this category are divided into eight main groups, including those using biometric identification, applied in critical infrastructure (e.g., transport), determining access to education or assessing students (e.g., exam scoring), used in law enforcement and judicial spheres, and others *(Petriv O., Available: http://surl.li/pucrl).*

The Ukrainian government has declared a path to its own AI development strategy and the formation of a progressive policy in the field of artificial intelligence and an agenda for the world. Today, AI is actively used in various directions in Ukraine. Ukraine has started work towards legal regulation of AI use. As a member of the Council of Europe's Ad Hoc Committee on Artificial Intelligence, in October 2019, Ukraine joined the Organization for Economic Co-operation and Development's Recommendations on Artificial Intelligence (OECD/LEGAL/0449).

In 2020, by the Cabinet of Ministers of Ukraine Decree of December 2, 2020, No. 1556-r *(Kontseptsiia rozvytku shtuchnoho intelektu v Ukraini. Available: http://surl.li/gtojq),* the Concept for the Development of Artificial Intelligence in Ukraine was approved, which, for the first time at the legislative level, provides a definition of artificial intelligence and sets out the goals, principles,

and tasks for the development of AI technologies in Ukraine. The implementation of the Concept's tasks is planned until 2030.

According to the Concept, AI is an organized set of information technologies that enable the execution of complex tasks through the use of a system of scientific research methods and information processing algorithms, obtained or independently created during work, as well as creating and using proprietary knowledge bases, decision-making models, information processing algorithms, and defining ways to achieve set tasks.

The Concept proclaims the development and use of AI systems only under the condition of the rule of law, fundamental human and citizen rights and freedoms, democratic values, and ensuring appropriate guarantees when using such technologies and implementing AI technologies in the fields of education, science, economy, public administration, cybersecurity, justice, defense, and other areas to ensure Ukraine's long-term competitiveness in the international market.

Among the recent developments towards standardizing the use of AI in Ukraine is the roadmap for regulating artificial intelligence in Ukraine *(Rehuliuvannia shtuchnoho intelektu v Ukraini. Available: http://surl.li/qmlmk),* developed by the Ministry of Digital Transformation. This roadmap is primarily aimed at supporting business competitiveness and ensuring access to global markets in terms of the scale of AI usage worldwide, while it also emphasizes the need for measures for the gradual integration of AI Act norms into domestic legislation.

Therefore, based on the above, let us try to take a brief excursion into the legal fields where, in our opinion, the standardization of AI usage will require priority decisions and/or such decisions are already being implemented.

Field of law - a set of relatively separate legal norms and institutions regulating and protecting a specific sphere of social relations characterized by qualitative uniqueness and unity (homogeneity). *(Entsyklopediia suchasnoi Ukrainy. Available: http://surl.li/qmlnq)*

First of all, let's turn to the general theory of state and law, namely the classical objects and subjects of law. The object of law is material and immaterial goods regarding which legal relations arise. The counterpart to the category of the object of law is the subject of law. The objects of law include: things, money, securities, and other property, including property rights; works and services; information; intangible personal goods (human honor and dignity, freedom, and inviolability, etc.); products of intellectual activity and intellectual property rights; behavior and actions of legal and natural persons. The types and scope of material and immaterial goods that constitute the objects of law are determined by the legislator and enshrined in laws and other regulatory legal acts. The concept of the "object of law" is practically identical to the concept of the "object of legal regulation". *(Entsyklopediia suchasnoi Ukrainy. Available: http://surl.li/qmlqj)*

Civil law. In this area, the cornerstone regarding the standardization of artificial intelligence is the dilemma of whether AI is a subject or an object of law? Discussions on this issue are ongoing, and in our opinion, they will only increase with the development of AI capabilities and its learning.

The issue of recognizing artificial intelligence and robots as new subjects of civil law is increasingly being raised among scientists, and there is currently no consensus on this issue. However, due to the continuous development of modern technologies, legal regulation in this area will also evolve.

The theory of the subject regarding artificial intelligence is associated with the use of the term "electronic person." Scholars who express this view regarding artificial intelligence emphasize the existence of individual subjective rights and obligations in such a person and civil legal capacity in general. Thus, in the doctrine of civil law, it is argued that electronic person has civil legal capacity, and therefore, there are all grounds to consider artificial intelligence a subject of civil law. It is also proposed to include "cyber capacity" in the list of types of legal capacity of legal entities – the ability to be an active participant in relations in the IT sphere. At the same time, "cyber capacity" can be realized not only through legal transactions but also through legal actions within the framework of special legal capacity of AI. The development of the doctrine of civil legal capacity of artificial intelligence is reasonable. As researchers emphasize, in October 2017, the "human-like robot Sophia was granted citizenship and thus became a citizen of Saudi Arabia, becoming the first robot to acquire legal personality in a certain country *(Zozuliak O. I., 2022).*

Nick Bostrom conducted research on the phenomenon of intelligent machines and concluded that by 2022, artificial intelligence systems would think approximately 10% as humans, by 2040 - 50%, and by 2075, thought processes would be indistinguishable from human ones *(Mylonenko Yu. V., 2018).*

We also recall the positioning of artificial intelligence in the Resolution of the European Parliament 2018/2088(INI) precisely as an "electronic person" *(European Parliament resolution. Available: http://surl.li/qmlxv).* The issue of expanding the circle of subjects of civil law is particularly interesting and debatable from the perspective of analyzing the Resolution of the European Parliament 2015/2103(INL), the provisions of which provide for a specific legal status for intelligent robots *(Floridi L., 2016).* According to the Civil Code of Ukraine *(Tsyvilnyi kodeks Ukrainy. Available: http://surl.li/kixz).* (Article 2. Participants of civil relations), the participants of civil relations are natural persons and legal entities. Participants of civil relations include: the state of Ukraine, the Autonomous Republic of Crimea, territorial communities, foreign states, and other subjects of public law. These entities are endowed with certain rights and obligations accordingly.

Directly in Ukrainian legislation, the types of objects of civil rights are also defined. According to Article 177 of the Civil Code of Ukraine, the objects of civil rights are things, money, securities, digital things, property rights, works and services, results of intellectual, creative activity, information, as well as other material and immaterial goods. Objects of civil rights can exist in the material world and/or in the digital environment, which determines the form of objects, features of acquisition, exercise, and termination of civil rights and obligations regarding them.

The current domestic legal regulation of artificial intelligence defines it as an object of law because it is inappropriate to equate artificial intelligence with living beings considering the current level of AI development since artificial intelligence in any of its embodiments is currently devoid of the ability to exercise subjective rights and legal obligations (devoid of legal capacity and legal capacity), as well as devoid of emotions. The reality is that any artificial intelligence is created by a human or group of humans. Therefore, it is the developers of AI who are responsible for the safety of its implementation and use and the potential infliction of property (material) and moral harm to others. AI can be sold or given as a gift, or any other actions provided for by civil legislation can be taken with this technology, freely alienated, or transferred from one person to another by way of succession or otherwise. Therefore, today AI technology is an object of the material world that may give rise to civil rights and obligations.

At the same time, in this matter, in our opinion, it is inappropriate to draw a conclusion. The speed of AI development and its learning is impressive, research into this technology is conducted on a global scale. Let's remember N. Stevenson, C. Clarke, A. Asimov, and V. Vinge with their predictions of the development of digital society, robots, and technologies. Therefore, the question of defining AI as a subject of civil law remains open, and therefore, work on it needs to be done now to timely respond to the challenges associated with the need for changes in domestic civil law due to the possibility of the emergence of a new type of legal entity.

The next relevant direction is copyright, and in this area, in our opinion, the domestic legislator has significantly advanced towards the legal regulation of AI. In 2023, the Law of Ukraine "On Copyright and Related Rights" dated December 1, 2022, No. 2811-IX *(Zakon Ukrainy «Pro avtorske pravo ta sumizhni prava». Available: http://surl.li/qmmbp)* entered into force. This law is an adaptation of legislation to the current state of technology development and an important step in regulating copyright in computer programs and databases. An interesting feature of the law is the introduction of the concept of "non-original objects" created by computer programs.

Non-original objects generated by a computer program (programs) are protected by a sui generis right under Article 33 of this Law. A non-original object generated by a computer program is an object that differs from existing similar objects and is formed as a result of the functioning of the

computer program without the direct participation of a natural person in the formation of this object. Works created by natural persons using computer technologies are not considered non-original objects generated by a computer program (for example, an article or book created by a person using ChatGPT).

Subjects of sui generis rights to non-original objects generated by a computer program may be persons who own property rights or have licensing authority for the computer program provided for in the first part of this article. As a result of the creation of a non-original object generated by a computer program, personal non-property rights do not arise.

The sui generis right to a non-original object generated by a computer program arises from the fact of generating this object and begins to operate from the moment of its generation. The term of validity of the sui generis right to a non-original object generated by a computer program expires after 25 years, calculated from January 1 of the year following the year in which the non-original object was generated. The law also provides for corresponding protection of rights, including judicial protection.

Criminal law. The issue of regulating AI in criminal law and civil law is similar. First of all, this issue concerns the recognition of AI as a subject or object. In criminal law, accordingly, the issue concerns the recognition of AI as a subject of a criminal offense or as an object of such an offense, a tool or means of its commission.

The following properties of artificial intelligence are highlighted: 1) the ability to process significant amounts of information obtained from various sources; 2) the ability to self-learn (including accumulating experience, generalizing, finding non-obvious connections) and reasoning; 3) planning skills; 4) the ability to contemplate (in response to developers' contemplations about it, artificial intelligence will spend more powerful resources contemplating them) *(J. Barrat, Available: http://surl.li/qmmgf).*

According to Article 18 (Subject of a Criminal Offense) of the Criminal Code of Ukraine, the subject of a criminal offense is a convicted natural person who committed a criminal offense at an age from which, according to this Code, criminal responsibility may arise. Above, we have already described the prospects for the development of AI, including its status as a legal entity and corresponding legal personality.

Granting artificial intelligence the status of an "electronic person" is unlikely to encounter objections or non-acceptance in the field of criminal law relations. After all, the fact of recognizing a legal entity as a subject of numerous legal relations, including criminal ones, is not controversial (Art. 96-3, 96-4, 96-6. Chapter XIV-1 "Criminal Law Measures Regarding Legal Entities" of the Criminal Code of Ukraine) *(Radutnyi O. E., 2017).*

Scientific literature describes the position regarding the possible inclusion in the Criminal Code of Ukraine of a section tentatively titled "Criminal Law Measures Regarding Electronic Persons," if the latter are not recognized as subjects of the crime with all subsequent legal consequences of such a systemic change *(Karchevskyi M., Radutniy O., 2023).* Next is the question of whether AI is an object or subject of a criminal offense, or a tool or means of its commission? According to domestic legal doctrine, the object of a crime is social relations, interests, goods protected by criminal law from socially dangerous encroachments, and to which harm is caused or the danger of such harm is created in the process of committing a crime.

The subject of a crime is an item of the material world about which or in relation to which a crime is committed, and with certain characteristics of which criminal law associates the presence in the actions of a person of signs of a specific criminal offense. In turn, the means of committing a crime are objects that the offender used to commit the crime and directly influenced the object, subject, or victim of the crime. These are objects that are directly used by the perpetrator to commit actions that constitute the elements of a completed crime, while the tools are only used to overcome obstacles in achieving the criminal goal *(Shalhunova S.A., 2019).*

Therefore, according to national legal doctrine, an artificial intelligence system can be considered an object of crime when it is a component of social relations protected by law. However, depending on the circumstances, AI can be used to commit a criminal offense or pose a direct threat to protected rights and legitimate interests of individuals, society, and the state.

Criminal law primarily describes the elements of a crime based on its objective side. The objective side of a crime is the set of legally significant features that characterize the external aspect of the crime, including: socially dangerous conduct (mandatory feature), socially dangerous consequence, causal connection between socially dangerous conduct and socially dangerous consequence, time, place, manner, circumstances, and means (tools) of committing the crime (optional features, which may be mandatory, qualifying, or privileged in the commission of a specific crime) *(Us O. V., 2018).*

Thus, considering the aforementioned circumstances, it is already advisable today to rethink the understanding of the place of AI in criminal law relations. The current norms of the Criminal Code of Ukraine require reconsideration in light of the fact that AI in its various embodiments is used in the commission of a significant percentage of criminal offenses, and the proportion of these offenses will increase: crimes in the field of national security, human trafficking, drugs and weapons trafficking, the banking sector, fraud, violations of electoral rights, and more. These are not exclusive categories of crimes in which AI is used.

Currently, there are numerous controversial issues in the practical application of the norms of the Criminal Code of Ukraine in this direction. One recent example is the draft law "On Amendments to the Criminal Code of Ukraine regarding the establishment of liability for electronic communication fraud"*(Vidpovidalnist za elektronno-komunikatsiine shakhraistvo. Available: http://surl.li/qmmsp)*, which proposes the introduction of additional norms, given the presence in the domestic Criminal Code of offenses provided for in Part 4 of Article 190, 200, 231, the norms of which do not meet the requirements of today in the field of illegal use of digital solutions.

Therefore, there is an urgent need to address this issue before the legal regulation of AI, taking into account the possible granting of the status of an "electronic person." It may be proposed to improve the norms of the Criminal Code of Ukraine for additional qualification of a criminal offense committed using AI as a tool or means. Currently, Article 361-1 (Creation for the Purpose of Illegal Use, Distribution or Sale of Harmful Software or Technical Means, as well as their Distribution or Sale) of the Criminal Code of Ukraine does not meet modern requirements, as it envisages a specific unlawful purpose. However, AI in its various embodiments is created with good intentions and later used to commit various categories of offenses. This issue becomes especially relevant in connection with the widespread use of AI in the commission of certain crimes, provided for in Chapter XX (Criminal Offenses against Peace, Humanity, and International Order) of the Criminal Code of Ukraine, for example, violations of international humanitarian law during armed conflicts when AI-powered weapons are used against civilian populations.

The use of artificial intelligence in procedural aspects (criminal and civil procedure). Clarifying the circumstances of committing a criminal offense and establishing the guilty party is an undeniable fact: AI technologies in the field of biometric verification/identification, input of biometric data, management of this data; alternative chatbots to counteract chatbots in the drug trade; technologies for predicting crimes and actions of potential offenders; profiling of offenders; expert examinations, conducting covert investigative (search) actions (CIA). The question of the application of AI in countering military aggression and investigating relevant crimes is particularly relevant. Artificial intelligence helps identify Russian military personnel, search for targets, intercept enemy communications, and is also an integral part of conducting propaganda and disinformation campaigns. This list of AI technology uses in the process of detecting and proving crimes is inexhaustible and will expand.

For example, let's mention the RICAS system - a real-time intelligence and crime analysis system *(RICAS. Available: http://ricas.org)*. RICAS allows for the following types of analysis: crime structure analysis, overall profiling analysis, specific investigation analysis, comparative analysis, analysis of offender groups, specific profile analysis, and investigation analysis. It is also worth

mentioning the software with AI elements "Cassandra," which will analyze the possibility of repeat offenses by a criminal. This assessment is carried out by an algorithm that assigns scores to various questions and then summarizes them. In a few years, there will be a large dataset, based on machine learning results, where "Cassandra" will learn to analyze not only responses to a list of simple questions but also all other data available about the criminal *(Shevchuk T.A., Svystun Ya.V., 2021.).*

However, unlike the Civil Procedure Code of Ukraine, the Criminal Procedure Code of Ukraine has not yet introduced the concept of electronic evidence. Instead, the Criminal Procedure Code of Ukraine *(Tsyvilnyi protsesualnyi kodeks Ukrainy. Available: http://surl.li/qmmzd)* defines electronic evidence as information in electronic (digital) form containing data about circumstances relevant to the case, including electronic documents (including text documents, graphic images, plans, photographs, video and audio recordings, etc.), websites (pages), text, multimedia and voice messages, metadata, databases, and other data in electronic form. Such data may be stored, in particular, on portable devices (memory cards, mobile phones, etc.), servers, backup systems, and other places where data in electronic form are stored (including on the Internet). The procedure for submitting such evidence, their evaluation, storage, and return are determined.

While the Criminal Procedure Code of Ukraine leaves procedural questions regarding the understanding of the status of evidence obtained through AI technology open, defining their relevance and admissibility, standardizing the procedure for obtaining evidence through the use of AI technology considering the specifics of various aspects of application (biometric identification of offenders and their profiling, determining the possibility of recidivism, CIA, expert examinations, and analytics, among others), procedural questions neutralizing potential risks to human rights associated with the use of AI technologies in evidence gathering remain unaddressed.

There is an urgent need to ensure:

1. Standardization of AI technology (specific DSTU or procedures).

2. Legal regulation of AI usage in the field of detection, documentation, and proof of criminal offenses.

Given this, it is advisable to start working towards standardizing all the above-mentioned issues, and it would be reasonable to develop a new section of the Criminal Procedure Code of Ukraine dedicated to this direction.

A separate topic in the process of legal regulation of AI is the protection of personal data. Currently, domestic legislation on personal data protection is outdated and does not fully ensure the protection of such rights in light of the development of international standards *(Zakon Ukrainy «Pro zakhyst personalnykh danykh». Available: http://surl.li/jria).* Therefore, due to the significant increase in digital technology activity, the legislator has identified several focuses in the draft Law

"On Personal Data Protection" (No. 8153 dated 25.10.2022) *(Proekt Zakonu «Pro zakhyst personalnykh danykh». Available: http://surl.li/qmnav)*. Among other things, the use of tracking technologies for personal data subjects' actions in electronic communications and services, features of profiling and automated processing of biometric data, and others are provided for, which in turn will contribute to standardizing AI in personal data processing and protection.

We have focused only on specific areas of law in the field of AI legal regulation, but today computer programs, information technologies based on artificial intelligence, such as various chatbots, generative platforms, virtual assistants, and works with the prospect of obtaining the status of an "electronic person," have become widely used in all spheres of life. Each of these manifestations of AI requires legal regulation with the establishment of clear boundaries and the filling of concepts, both in general and in specific areas of application. Therefore, a clear and understandable conceptual-categorical apparatus is needed. Currently, Ukrainian legislation contains several legal acts, in addition to the Concept, that contain terms relevant to understanding AI: the Law of Ukraine "On Basic Principles of Ensuring Cybersecurity of Ukraine," the Law of Ukraine "On Electronic Communications," the Law of Ukraine "On Information Protection in Information and Communication Systems." The list of terms and definitions is quite extensive, including information technologies, computer programs, robots, electronic communication technologies, electronic communication network, and others.

The issues discussed and the author's assessment provided are certainly debatable and open to wide discussion given their relevance. However, it is permissible to propose certain conclusions regarding further steps in AI legal regulation:

– Formulate a legal regime overall for the use of artificial intelligence, which will subsequently necessitate the creation of a legal regime for the application of AI in a specific field;

– Develop a conceptual-categorical apparatus for AI usage overall, and subsequently considering a specific field of law;

– Establish criteria for maintaining a balance between administrative regulation and free access to AI in the interests of societal and state development;

– Provide regulatory regulation of the peculiarities of personal data processing using AI technology and protection of such data;

– Develop a framework regulatory act (law) on artificial intelligence, which will define the legal and organizational foundations of state policy in the field of AI usage, as well as the rights, duties, and responsibilities of individuals and legal entities participating in the relevant activities or using AI;

– Furthermore, ensure amendments to domestic legislation in relevant areas of law, with detailed provisions on the use of AI, taking into account the peculiarities of the social relations regulated by a particular regulatory act.

I.4. Environmental challenges and the contribution of AI to their resolution. Even if the world adheres to the commitments of the Paris Agreement, the temperature in the Arctic is projected to continue rising by 3-5°C by 2050, as summarized by the UN Environment Report *(Available: http://surl.li/qmnka).* Glacier melting will lead to sea-level rise and threaten four million people and approximately 70% of the current Arctic infrastructure. The report emphasizes the need for decisive measures to reduce emissions.

According to the World Economic Forum report 'Using Artificial Intelligence for Earth' *(Vsesvitnii ekonomichnyi forum. Available: http://surl.li/qmnlr)* artificial intelligence (AI) refers to computer systems that 'can perceive their environment, think, learn, and act according to their programmed goals.' On a city scale, AI can improve overall energy efficiency by incorporating data from smart meters and other devices to forecast the city's energy needs. This will help municipal service providers optimize energy production, effectively reducing their climate impact.

Additionally, technology providers are actively developing AI-based modeling tools. For example, IBM has developed a program to help cities predict heatwaves. The program models the climate on a city scale and explores different strategies to test which ones will best reduce heatwaves. For instance, if a city wants to plant new trees, machine learning-generated models can determine the best locations for planting to create optimal tree cover and reduce heat from sidewalks.

Artificial intelligence can be used to achieve a variety of critical tasks for humanity:

– Creating new low-carbon materials to replace steel and concrete.

– Timely prediction of extreme weather conditions for appropriate responses.

– Monitoring deforestation through satellite imagery.

– Transforming natural clouds or creating artificial clouds using aerosols to reflect more solar heat back into space *(Shtuchnyi intelekt (ShI) na zakhysti klimatu, ekolohii ta bioriznomanittia. Available: http://surl.li/qmnoa).*

Despite the global positive aspects of using AI in the field of ecology, concerns about the danger of using AI are also voiced. For AI to perform its tasks, it needs to master vast amounts of data. To learn to recognize a car, an algorithm must sift through millions of images of cars. ChatGPT processes huge textual databases to learn to work with human language.

Data processing takes place in data processing centers (DPCs). It requires significant computational power and is very energy-intensive. 'Two to four percent of global CO2 emissions

come from the entire infrastructure of such data centers and data transmission networks. This is approximately the same as emissions from aviation transport.'

In a 2019 study, scientists from the Massachusetts Institute of Technology calculated that 'training' one large AI device could result in emissions of up to 284 tons of CO2 equivalent - almost five times more than the emissions from a car throughout its production and operation period *(Miuller N., Available: http://surl.li/qmnqj).*

Contrary to criticism, scientists have proven that AI-based technologies can provide users with more opportunities to reduce their own carbon footprint. These include various smartphone applications or other technological solutions that help calculate users' individual contributions to overall greenhouse gas emissions and provide practical recommendations for reducing these contributions, such as reducing meat consumption, using public transport instead of a private car, economical electricity consumption at home or in the office, etc. Artificial intelligence, with reasonable approaches, will become a powerful assistant in combating climate change *(Rolnick D., Available: http://surl.li/qmnrr.)*, which is a threat to human existence.

At the end of 2019, a group of researchers in the field of artificial intelligence presented a comprehensive scientific work entitled 'Machine Learning for Combating Climate Change.' This work thoroughly examined 13 areas (from utilities to agriculture and manufacturing) where AI algorithms can help humanity in combating climate change and challenges.

Electric power systems. Artificial intelligence is often referred to as the new electricity due to the immense potential of this technology to transform many different sectors. Interestingly, the electric power supply system itself is one of the areas that artificial intelligence can transform in the near future.

Today, electric power systems account for about a quarter of all human-induced greenhouse gas emissions. Machine learning technologies can help reduce emissions from power generation systems by accelerating the development of clean energy technologies, improving forecasts of energy demand and clean energy generation volumes, and through overall optimization of energy production management and monitoring systems.

Transportation. The transportation sector is responsible for a quarter of all carbon emissions and currently shows no trends of emission reduction. Two-thirds of transportation emissions come from road travel, with aviation showing the highest emission intensity and fastest growth.

With artificial intelligence technologies, we can improve the design of transportation vehicles, build more thoughtful infrastructure, optimize public transportation schedules, assist in the development of shared mobility systems, shift transportation from roads to rail, which is the most efficient in terms of greenhouse gas emissions.

Residential and municipal sector. Energy used by buildings accounts for a significant portion of emissions. By implementing several relatively easy-to-implement solutions, emissions from buildings can be reduced by 90%.

Artificial intelligence technologies can provide critical tools for managing energy consumption in individual buildings and shaping energy efficiency policies for entire cities. Various machine learning techniques can help develop solutions that will be most effective for specific buildings and ensure the implementation of these solutions through appropriate "smart" systems. At the urban planning level, neural networks can gather and process vast amounts of data to make more informed decisions in the city-building process.

Manufacturing. Industrial production, logistics, and construction materials are the main causes of emissions that are difficult to eliminate. Fortunately, thanks to the efforts of artificial intelligence researchers, the industrial sector spends billions of dollars annually collecting data on the activities of plants, factories, and logistics systems. Such volumes of information have become accessible, and thanks to the implementation of new data collection mechanisms via QR codes and image recognition.

Thus, thanks to the availability of large amounts of data and access to cloud environments for storing and processing information, the industry can become an ideal place to demonstrate the positive effect of machine learning on climate change. The work of artificial intelligence experts can potentially reduce global emissions by streamlining supply chains, improving product quality, predicting breakdowns, and optimizing heating and cooling systems.

Agriculture. Greenhouse gases are emitted not only by engines and factories, but a significant portion of harmful emissions is the result of farming activities. In modern agriculture, the practice of growing a single crop over a large area of land predominates. This approach simplifies farm management but simultaneously leads to a decrease in soil nutrients and, accordingly, a decrease in its productivity. As a result, many farmers begin to actively use nitrogen-based fertilizers, which can convert into nitrous oxide - a greenhouse gas that is 300 times more potent than carbon dioxide.

Artificial intelligence algorithms can help farmers combine different crops more effectively, better predict when to plant certain crops, as well as which crops will help restore soil fertility, and consequently reduce the need for fertilizers.

Full-scale application of artificial intelligence in agronomy is already the nearest future. According to the conclusions of the U.S. National Institute of Food and Agriculture, machine learning can effectively analyze crop conditions, identify problems and their locations in the field, target the application of plant protection agents, reduce environmental impact, decrease the amount of fertilizers and water used by using them in the necessary quantity. As an example, the activities of Corteva

Agriscience, a global agricultural company, are aimed at working with farmers to develop more useful and powerful technologies. The company's researchers use Google Cloud solutions in many areas of their work, including research and development, data processing, and plant breeding departments. The company's digital technology department has utilized tools from Google Cloud and partner Kin + Carta for photometry - a project that uses artificial intelligence to forecast corn yield to plan necessary agronomic work. Corteva's mobile photometry uses machine learning, artificial intelligence, and a small amount of user data (plant density and weight of 1000 seeds) to accurately adjust corn yield measurements in the field *(Kovalenko O., Available: http://surl.li/qmnzn).*

Ukrainian researchers, despite the difficulties caused by armed aggression, are not lagging behind their colleagues in researching AI in addressing environmental threats *(Ukrainskyi hidrometeorolohichnyi instytut. Available: http://surl.li/qmoaz).* On September 18, 2023, the 78th session of the United Nations General Assembly took place. As part of the event "Artificial Intelligence to Accelerate Progress in Achieving Sustainable Development Goals," scientists from the Ukrainian Hydrometeorological Institute (UkrHMI), the State Emergency Service of Ukraine, and the National Academy of Sciences of Ukraine, in collaboration with IBM Research and Texas Agrilife Research, presented a joint environmental project.

Scientists from UkrHMI presented two online platforms, "Land & Water" and "AgroStats," through which any interested parties, environmental experts, farmers, government bodies, can obtain information on drought forecasting, water resource management, and agricultural statistics of Ukraine. These platforms are relevant due to the constant destruction of critical infrastructure in the country. They will enable making informed decisions to protect Ukraine's agriculture and water resources for future generations.

These platforms, based on AI, contribute to the achievement of the Sustainable Development Goals (SDGs) declared by the UN:

- SDG 2 - Zero Hunger,
- SDG 6 - Clean water and Sanitation,
- SDG 13 - Climate action.

Science and practice go hand in hand in researching the prospects of using AI in combating environmental hazards *(Call for Submissions. Available: http://surl.li/qmoch).* The University of Cambridge has established a new center focused on developing ways to use artificial intelligence to mitigate environmental risks. The center will focus on developing "new methods for utilizing AI potential for analyzing complex environmental data and thus planning sustainable paths for the future" and ongoing projects of similar scope, including those aimed at using AI to understand earthquake risks and monitor active volcanoes.

NASA, IBM, and HuggingFace have initiated cooperation to create a next-level artificial intelligence model that will help scientists track climate change, forest conditions, air quality, and other environmental aspects. According to NASA's estimates, within the Earth science program, about a quarter of a million terabytes of data will be generated in 2024. To enable scientists to effectively process these vast amounts of raw satellite data, IBM, HuggingFace, and NASA will create an open-source geospatial database that will serve as the foundation for a new class of AI capable of tracking deforestation, predicting crop yields, estimating greenhouse gas emissions, and more. For this project, IBM is applying the recently released Watsonx.ai as the base model, utilizing a year's worth of harmonized data from NASA Landsat Sentinel-2 satellites. These data are collected by a pair of ESA Sentinel-2 satellites designed to capture high-resolution optical images over land and coastal areas in 13 spectral bands. In turn, HuggingFace has hosted the database on its open-source AI platform. According to IBM, by precisely tuning to "data for mapping scars from floods and fires," the team was able to improve the model's performance by 15%, while using half the amount of data. By applying flexible, reusable AI systems with data repositories from NASA satellites and hosting them on the leading open-source AI platform, Hugging Face, the power of collaboration will be leveraged to deliver faster and more efficient solutions in the field of ecology *(Available: http://surl.li/jtjnh).*

In conclusion, it should be noted that artificial intelligence and ecology are simultaneously independent and closely interconnected directions of societal development, this is our reality. Ahead of us are resilient AI models capable of skillfully modeling and understanding challenges in the field of ecology and contributing to their mitigation. For the effective implementation of AI technology in the field of ecology, work is needed on both technical solutions and addressing administrative and legal aspects. This involves setting new standards, harmonizing terminology and methodologies, and regulatory framework for all the solutions and innovations that already exist and will be created due to the prospects of AI in ecology.

Ukraine is currently in an extremely difficult situation due to military aggression, and the consequences for Ukraine's ecology are catastrophic. Burned forests and fields, polluted rivers and soil, flooded cities and villages are among the visible effects. According to the State Environmental Inspection, as of January 2023, the losses for Ukraine's ecology due to 11 months of Russian military aggression amount to over 1 trillion 743 billion hryvnias, or over 47.6 billion dollars. And these are only approximate calculations, as a part of Ukrainian territories remain occupied *(Pohliad z suputnyka. Available: http://surl.li/mkgmr).*

Artificial intelligence can be a solution to overcome these challenges. Despite the situation in the country, active work in this direction is necessary today. The creation and functioning of a state

environmental monitoring system and its subsystems, a nationwide environmental automated information-analytical system to support decision-making and access to environmental information, and interaction of its sectoral components are planned. The positive impact of using AI technology in implementing these tasks is undeniable.

The establishment of this system is regulated by the Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine Regarding the State Environmental Monitoring System, Environmental Information (Environmental Information), and Information Support for Environmental Management" dated March 20, 2023, No. 2973-IX *(Available: http://surl.li/qmoev).* This Law comes into force six months from the date of cancellation or termination of the state of war, except for the provision that comes into force from the day following the publication of this Law, which sets tasks for the Government of the country within one year from the date following the publication of this Law to ensure the adoption of regulatory acts provided for by this Law and bring its regulatory acts into compliance with it.

The problem is that military aggression may continue, and environmental issues require immediate resolution, so active work in searching for automated solutions and implementing AI technologies to overcome environmental threats caused by the consequences of military aggression is necessary today.

Overcoming environmental threats and challenges involves the implementation of AI through the creation of various analytical systems and integrated online systems, including those to European and other international platforms, for analysis and information provision to state institutions and other users to support decision-making in the field of environmental protection and restoration, as well as planning measures to prevent harmful changes, planning and obtaining international assistance. Currently, various mobile applications in the field of public interaction and various law enforcement agencies have proven themselves positively, for example, those introduced by the Security Service of Ukraine and the national police to inform citizens about violations of the law, movement of aggressor forces, and informing about the danger of mined territories. Therefore, it would be appropriate to use mobile applications with the ability to alert law enforcement agencies about unlawful activities in the field of the environment (pollution, poaching, deforestation, illegal dumps, etc.).

I.5. Information Security and Counteracting Cyber Threats. The use of artificial intelligence (AI) in the context of cybersecurity is becoming an increasingly important aspect of ensuring international security. AI can make a significant contribution to preventing cyberattacks, detecting threats, and responding to them, thereby helping to reduce risks for countries and

international organizations. Several key aspects of using AI for cybersecurity within the framework of international security include:

1. *Threat Detection*: Using machine learning algorithms to analyze large volumes of data and detect anomalous activity that may indicate potential cyber threats. Monitoring network traffic and system logs to detect malicious actions and potentially harmful programs.

2. *Attack Prediction*: Developing predictive models based on historical data and trend analysis to forecast future cyber threats. Using analytics to identify possible attack scenarios and determine the most probable attack vectors.

3. *Defense Against Attacks*: Utilizing artificial intelligence to automatically detect and block malicious programs and malicious traffic. Developing access management and authentication systems that use analytical methods to detect anomalous user behavior.

4. *Recovery After Attacks*: Using analytical tools to assess damages after cyberattacks and develop recovery strategies. Automated analytics help identify weaknesses in the system and develop action plans in case of access loss or security breaches.

5. *International Cooperation*: Using artificial intelligence to analyze global trends in cybersecurity and collaboratively respond to threats with other countries and international organizations. Sharing information and training machines to detect and respond to cyber threats in real-time.

The overall goal of using artificial intelligence in cybersecurity is to ensure international stability and protection against cyber threats on a global scale.

I.6. Psychological Aspects of Human Interaction with AI Systems. For the user, generative artificial intelligence (AI) appears to be superhuman or at least significantly enhanced in cognitive terms. To the naive user, it appears as an incredibly fast and precise scientific librarian combined with a erudite professor. It facilitates the synthesis and exploration of global knowledge much more efficiently than any existing technological or human interface, doing so with unique comprehensiveness. Its ability to integrate diverse realms of knowledge and simulate various aspects of human thinking makes it erudite to such an extent that it surpasses the ambitions of any highest-level human group. However, at the same time, it has the ability to misinform its human users with incorrect statements and outright fabrications.

The long-term significance of generative artificial intelligence extends beyond commercial implications or even non-commercial scientific breakthroughs. It not only generates answers but also raises philosophically profound questions. It will influence diplomacy and security strategy. However, none of the creators of this technology are addressing the problems it will create itself.

Even if generative artificial intelligence models become fully interpretable and accurate, they will still create problems inherent to human behavior. This may have certain consequences. As people rely less on their brains and more on their machines, they may lose some abilities. Our ability to think critically, write, and (in the context of text-to-image conversion programs like DALL-E and Stability.AI) constructivism may atrophy. The impact of generative artificial intelligence on education may manifest in a decrease in the ability of future leaders to distinguish what they understand intuitively from what they mechanically learn. There is an urgent need to develop a sophisticated dialectic that allows people to challenge the interactivity of generative artificial intelligence, not just substantiating or explaining the answers of artificial intelligence, but also questioning them. To curb our societal dependence on machines as arbiters of reality, strict cultural norms will be necessary rather than legal bans.

It is important for people to develop confidence and the ability to doubt the results of artificial intelligence systems *(Henri Kissindzher, Erik Shmidt, Daniel Huttenlokher. Available: http://surl.li/qmojk).*

Among the main advantages of artificial intelligence are:

1. *Disease diagnosis*. According to research by the international analytics agency Global Market Insights, from 2017 to 2024, annual growth in the use of artificial intelligence in healthcare is expected to reach 40%. That is, the impact of artificial intelligence on medicine will increase by almost half. Artificial intelligence technologies are already used in disease diagnosis, genome research, and drug development. They allow for more qualitative provision of information, patient servicing, time and cost savings.

2. *Legal sphere*. Artificial intelligence technologies are used in law enforcement. These include judicial and law enforcement registries, databases, systems that can identify a person, provide the necessary requested information about them, and so on.

3. *Analysis and processing of large volumes of data in all areas of industry, economy, and other spheres*. No person can receive, analyze, and give a clear result as much, as quickly, and as accurately as artificial intelligence. If a person can make mistakes in calculations, taking into account the human factor, then artificial intelligence is programmed to provide the most correct answer in the shortest possible time.

4. *Assistance of artificial intelligence technologies in the space industry and science*. Scientists have developed virtual intelligent assistants called CIMON to help astronauts identify dangers during long space flights, malfunctions in a spacecraft. For planning a mission to Mars and being there directly due to the limitation and unavailability of complete information, artificial

intelligence is the only reasonable system that can help. Artificial intelligence technologies can be used where a person physically cannot be or it would be dangerous.

5. *Time saving*. Artificial intelligence does not need to be taught at all - it is already programmed to perform certain types of work, unlike a person.

6. *Cost savings and efficiency of use in the banking sector*. Artificial intelligence helps in detecting fraud in the banking sector, as well as in the development of investment policy. Banks have AI-based software systems that help prevent money laundering.

On the other hand, we have threats of artificial intelligence:

1. *Mass unemployment*. It can cause an economic crisis, conflicts, a path to lawlessness and crimes.

2. *Loss of control over artificial intelligence*. Creating artificial intelligence with a human brain model can cause uncontrollability of robots by humans. This is all in the distant future, as it seems to us, but we see a rapid development of robot-like technologies that directly affect human life.

3. *Development of conflicts on religious, social, and economic grounds*. Given the above, there is no single opinion and reliably correct statement regarding the positive or negative impact of artificial intelligence on humanity. AI technologies can both help humans achieve another scientific and technological revolution and become a threat. They provide society with the necessary elements for life, thereby making it vulnerable and dependent *(D. Makhnenko. Available: http://surl.li/aikch)*.

To address many of the challenges associated with interacting with modern technical systems, especially after the emergence of specific "technophobias," it is important to understand that no machine can think like a human or act like a human (in terms of lacking motivation and goal-setting as such). The attempt to create an intelligent, primarily human-like entity has led to the formation of numerous anthropomorphisms regarding various technical systems within a certain part of human society. People have begun to interpret the activity of a machine from the perspective of their own activities and the value-motivational determinants underlying them. This provides an answer to the question of the emergence of artificial intelligence as a social-psychological phenomenon.

The creation of a "human-like machine" aimed not to open up a technical space for evolution to humanity, so the machine was endowed with human traits to overcome the psychological barrier of further symbiosis. In the distant future, machines will have human-like properties: motivation, values, needs precisely because this symbiosis is supposed to happen, but for now, these philosophical-anthropological quests are the subject of futuristic predictions of the distant future. However, people have already begun to perceive smart technologies from the standpoint that they can still "take revenge on humanity," "seize power" precisely through excessive extrapolation of their own personality traits onto objects that cannot have these traits in any case. And the more intelligent

machines become similar to their creators, the more anthropomorphism manifests itself in the world of information technology. Technophobia as unfounded fears or feelings of hostility towards technology and automation have various reasons for their emergence, with the most common associated with the objective understanding of the loss of jobs against the backdrop of the rapid replacement of human labor with automated machine work. This raises many ethical problems related to the limits of AI usage and its impact on human private life.

However, no technical system can do without humans as a source of queries and a source of knowledge. It has been found that generative artificial intelligence turned out to be an imitation, and in the field of content creation, it can combine, make substitutions, and reconstruct, but it is not capable of the creative process itself. This conclusion was reached by experts from Microsoft, Delft University of Technology, the Royal Mauritshuis Gallery, and the Rembrandt House Museum in Amsterdam while working on "The next Rembrandt" project.

Understanding the origins of artificial intelligence technologies allows us to understand their primary purpose - to free humans from excessive routine. However, human perception of this technological process has been enriched with unnecessary ideological notions, transforming mathematical algorithms into entities that they were not and could not be. Humanity must be prepared for changes in the labor market, a decrease in the share of labor in sectors that are already intensively being developed by machine learning algorithms: the field of mathematical calculations, linguistic translation, programming. This does not mean that humanity is on the brink of mass unemployment, but it will enable the application of human labor in cases where its expediency will be determined by purely human exclusivity *(Kyrychenko V. V., 2023)*.

Modern artificial intelligence research provides an opportunity to identify a specific set of features common to natural and artificial intelligence, as well as to identify the main parameters for their evaluation *(Derevianko S. P., Prymak Yu. V., Yushchenko I. M., 2020)*.

Parameters of evaluation	Key characteristics	
	Human intelligence (HI)	Artificial intelligence (AI)
Information analysis	For humans, it is anticipated to perform sequential, logical actions in interpreting acquired knowledge.	AI can analyze environmental information using sensors (motion, sound, light, etc.). One of the capabilities of AI is computer vision - AI technologies for real-time collection and analysis of video information.
The ability to reason	This ability in humans is associated with the process of thinking and is manifested in certain interconnected	One direction of AI is modeling reasoning, which involves creating symbol systems where a specific task is

	judgments aimed at determining the truth of a particular thought.	inputted, and the expected output is its solution.
Learning ability	In humans, this manifests in the ability to develop one's abilities and seek solutions in new situations.	One of the fields of AI is machine learning, which is the process of an intelligent system independently acquiring knowledge during its operation.
Self-learning	Human intelligence involves the orientation of activities towards independent acquisition of knowledge and experience.	A promising research direction is self-learning in AI, which involves the development of machine learning algorithms through the modification of SOINN (Self-Organizing Incremental Neural Network).
Language understanding	Language understanding involves extracting various types of information from an input linguistic signal, including the content of the message, the identity of the speaker, the language being spoken, as well as the emotional or psychological state of the speaker.	One of the directions of AI is natural language processing, which deals with the computer analysis and synthesis of natural language.
Emotion recognition	In humans, there is a process of perceiving, interpreting, and understanding the expressive manifestations of other people.	In the early 21st century, emotional computer systems (or emotional AI) were developed – devices capable of recognizing, interpreting, processing, and simulating human emotions.

The main common characteristics of natural and artificial intelligence include information analysis, reasoning ability, learning capability, self-learning ability, language understanding, and emotion recognition. However, human intelligence and artificial intelligence significantly differ in the results of their functioning (humans may exhibit a wider range of abilities, while machines may demonstrate greater intensity of these abilities) and motivational aspirations (actions by humans are purposeful).

The efforts of scientists to maximize the resemblance of artificial intelligence to human intelligence have led to the introduction of the concept of "emotional artificial intelligence" - intelligent systems capable of recognizing human emotions, interpreting them, and reacting to them adequately. In practical terms, emotional artificial intelligence is most promising in the social and medical fields. Modern social robotics is equipped with auxiliary tools for the interaction of emotional robots with people with disabilities and the elderly.

In turn, we believe that despite humanity's fears and the debate over the interaction between AI and humans, the implementation of AI in various spheres of life will contribute to human psychological comfort. This is because AI technology will enhance the duration and quality of life through the modernization of medical services (bioengineering, nanomedicine); the possibility of quality education; increasing individual safety through improved security environments; enhancing work efficiency and productivity; improving citizen-state interaction through the implementation of AI innovations, and consequently saving resources and time.

II. Artificial Intelligence and the Modern Smart State

II.1. The Main Principles of a Smart State. A smart state is a governance concept that relies on innovative technologies and data to improve citizens' lives, streamline government operations, and ensure the effective functioning of all sectors of society. The key principles of a smart state include:

– *Digitization:* Actively leveraging digital technologies for the transition to electronic governance, a digital economy, and digital services for citizens.

– *Innovation*: Encouraging the development of innovations and technological startups to accelerate economic development and enhance quality of life.

– *Open Data*: Providing access to open government data to increase transparency, accountability, and public participation.

– *Effective Governance*: Using data analytics to make informed decisions and optimize government processes.

– *Cybersecurity*: Ensuring the protection of critical infrastructure and data from cyber threats.

– *Citizen Engagement*: Creating mechanisms for active citizen participation in decision-making and policy formation.

– *Sustainable Development*: Working towards creating resilient and sustainable systems that address current needs while considering future generations.

– *Environmental Sustainability*: Focusing on the development of eco-friendly technologies and reducing carbon footprint to ensure environmental sustainability.

These principles aim to create an intelligent and innovative governance system that meets the requirements of modern society and contributes to its sustainable development.

II.2. The Impact of AI on the Formation of Smart States. Qualitative changes in the use of network digital technologies over the past decades have led to the identification of four stages of the digital revolution:

The first stage of the digital revolution (1990-2000) was characterized by the formation of necessary infrastructure to provide access to information via the Internet, with websites primarily intended for reading (receiving) information rather than posting and promoting it.

During the second stage (2000-2010), users personally became active participants in creating and accumulating data.

The third stage (2010-2020) was marked by the era of social networks and messengers (applications for instant messaging).

The fourth stage involves the construction of the so-called neural network, where communications between people, animals, and things will be based on principles of neurocommunication, utilizing artificial intelligence and the ubiquitous Internet of people, things, data, processes, etc *(Liashenko V.I., Vyshnevskoho O. S., 2018).*

Thus, the transition to the fourth stage, which includes extensive use of AI, is currently underway. Naturally, these processes, like any change, have two sides, as we mentioned above while analyzing the prospects of AI technology application in various spheres of society and state existence. These include risks in the field of human rights protection, technological and environmental hazards, economic troubles, including increased unemployment. However, we have also described the massive positive consequences of the prospects of implementing AI technology. Timely regulatory control of AI will ensure the protection of human rights and freedoms, AI technology will protect the environment and enable the development of medical care and treatment of severe diseases, and alongside the disappearance of certain professions, the introduction of AI will lead to the emergence of new ones.

Therefore, the task of a smart state in ensuring a comprehensive approach to the implementation of AI in all spheres of societal development, anticipating existing challenges, as well as developing and providing consultative and technological support in the implementation and use of AI technology.

For the effective and healthy transformation of society through the implementation of AI, while respecting democratic human rights and the rule of law, it is considered necessary to adhere to a number of principles in using AI in a smart state:

1. The principle of equal rights and opportunities for access to AI technology. Equal access to AI technology should be ensured for everyone in accordance with the requirements of legislation, information, and knowledge provided on the basis of such technology.

2. The principle by which AI will be used to create positive changes in various spheres of existence of the smart state and its population. This principle involves improving the quality of

healthcare and education services, creating new jobs, developing entrepreneurship, agriculture, transportation, environmental protection, ensuring a safe environment, and public safety.

3. The next principle is that the implementation of AI will contribute to the economic development of the smart state through increased efficiency and productivity, the acquisition of new competitive qualities and properties in various sectors of the economy, and accordingly competitiveness in the global market.

4. The principle of legal regulation, according to which the implementation of domestic standards for AI use in various industries will be ensured, of course, taking into account international experience, as well as ensuring regulatory regulation of AI technology use by adopting appropriate legislation.

5. The principle of information and cyber security, according to which the smart state, through legal, administrative, and organizational measures, ensures simultaneous development of AI technology in society and prevention, elimination, and management of challenges and risks in the fields of information security, cybersecurity, protection of personal data, privacy, and user rights of AI.

Thus, the task of a smart state on the path to widespread AI implementation is comprehensive state management of these processes, overcoming institutional and legislative barriers, launching national-level AI implementation projects, attracting relevant investments, stimulating the scientific community and business to develop AI technologies, coordinating market mechanisms in the field of AI use. A smart state must lead the processes of AI implementation and ensure their regulation.

II.3. Challenges and Development Prospects. The implementation of AI in various spheres of society will largely depend on the regulatory policies of the state and the creation of favorable conditions. The directions in which a smart state can influence the implementation of AI are quite broad, ranging from ensuring legal protection to investment. The main tasks of a smart state should include: regulatory regulation, including standardization in various fields of AI application, formation of AI usage culture, funding research in this area, and formation of new platforms for AI application.

Strategic decisions on the implementation of AI in a smart state include:

1. Government and state institutions' leadership in the development of artificial intelligence in all areas of public life.

2. Elimination of regulatory barriers hindering the implementation and development of AI.

3. Introduction of incentives and motivations for businesses, industries, and the economy as a whole to encourage them to transform their activities through the adoption of AI technology.

4. Creation and development of infrastructure for AI usage in everyday life.

5. Stimulating demand for AI technology from citizens and implementing national infrastructure projects based on principles of public-private partnership (in education, science, medicine, transportation, etc.).

6. Development and stimulation of AI usage in entrepreneurship by creating conditions for innovative activities through the implementation of appropriate financial and administrative mechanisms.

7. Development and deepening of citizens' competencies in the field of AI application, shaping society's and citizens' needs for the use of such technologies.

Conclusions. In light of the foregoing, based on the analysis conducted, the following main conclusions can be drawn. The use of artificial intelligence (AI) in international security systems is an important component of security assurance strategies, particularly in the context of the emergence of the 'smart state' concept. AI demonstrates effectiveness in detecting, predicting, and countering cyber threats, as well as optimizing various processes such as border control, early conflict prevention, humanitarian assistance, and crisis response. AI is a powerful tool that can optimize and improve all aspects of security discussed in the article.

It is also worth noting that the article highlights both the advantages and potential risks of using AI in the security field, as well as identifying prospects for its further development. Special attention is paid to the importance of legal regulation of AI use, particularly in Ukraine, as well as the protection of democratic human rights in the context of access to this technology. Psychological aspects of AI-human interaction, as well as strategic decisions regarding AI implementation in a smart state, are considered key aspects in the article.

The overall goal of the article is to promote understanding of the importance and potential of AI usage in the field of international security, as well as to develop recommendations for its effective utilization considering legal, ethical, and psychological aspects.

References:

Predicting conflict and humanitarian impacts | VIEWS. [Online]. Available: http://surl.li/qljwd. Accessed on: 15.02.2024.

J. Walter, P. Gutjahr, P. Nolz, “Multicriteria optimization in humanitarian aid”, European Journal of Operational Research, 252 (2016), pp. 351–366. [Online]. Available: http://surl.li/qlkar. Accessed on: 15.02.2024.

Z.Tazrout, “Artificial intelligence for border control and management: Focus on Frontex report”. [Online]. Available: http://surl.li/qlkhf. Accessed on: 15.02.2024.

Detecting, identifying, and reacting to threats in real-time. [Online]. Available: http://surl.li/qlkio. Accessed on: 15.02.2024.

New Technologies and the Protection of Civilians in UN Peace Operations. [Online]. Available: http://surl.li/qlklu. Accessed on: 15.02.2024.

Pravove rehuliuvannia Shtuchnoho Intelektu. Komitet tsyfrovoi transformatsii Verkhovnoi Rady Ukrainy. Holos Ukrainy vid 08.08.2023 r. [Online]. Available: http://surl.li/qlkpe. Accessed on: 10.02.2024. (In Ukrainian)
Artificial Intelligence Act. Brussels, 21.4.2021 COM(2021) 206 final 2021/0106(COD). [Online]. Available: http://surl.li/fooxn. Accessed on: 08.02.2024.
O. Petriv, "Shtuchnyi intelekt ta Artificial Intelligence Act: chas dlia yurydychnykh ramok", Tsentr demokratii ta verkhovenstva prava. [Online]. Available: http://surl.li/pucrl. Accessed on: 08.02.2024. (In Ukranian).
Kontseptsiia rozvytku shtuchnoho intelektu v Ukraini. Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 02.12.2020 r. № 1556-r. [Online]. Available: http://surl.li/gtojq. Accessed on: 11.02.2024. (In Ukranian).
Rehuliuvannia shtuchnoho intelektu v Ukraini: prezentuiemo dorozhniu kartu. [Online]. Available: http://surl.li/qmlmk. Accessed on: 11.02.2024. (In Ukranian).
Entsyklopediia suchasnoi Ukrainy. [Online]. Available: http://surl.li/qmlnq. Accessed on: 11.02.2024. (In Ukranian).
Entsyklopediia suchasnoi Ukrainy. [Online]. Available: http://surl.li/qmlqj. Accessed on: 11.02.2024. (In Ukranian).
O. I. Zozuliak, "Shtuchnyi intelekt yak obiekt tsyvilno-pravovoho rehuliuvannia", *Materialy mizhnarodnoi naukovopraktychnoi konferentsii, prysviachenoi pamiati prof. V. P. Maslova*, Kharkiv, liutyi, 2022. pp. 95–102. [Online]. Available: http://surl.li/qmltf. Accessed on: 12.02.2024. (In Ukranian).
Yu. V. Mylonenko, "Perspektyvy vyznannia shtuchnoho intelektu yak subiekta mizhnarodnoho prava", *Molodyi vchenyi*, №11, pp. 125–127, 2018. (In Ukranian).
European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI)). [Online]. Available: http://surl.li/qmlxv. Accessed on: 12.02.2024.
L. Floridi, "On Human Dignity as a Foundation for the Right to Privacy", *Philosophy & Technology*, P. 308, 2016. [Online]. Available: http://surl.li/qmlzd. Accessed on: 12.02.2024.
Tsyvilnyi kodeks Ukrainy. [Online]. Available: http://surl.li/kixz. Accessed on: 12.02.2024. (In Ukranian).
Zakon Ukrainy «Pro avtorske pravo ta sumizhni prava». [Online]. Available: http://surl.li/qmmbp. Accessed on: 12.02.2024. (In Ukranian).
J. Barrat, "Our Final Invention: Artificial Intelligence and the End of Human Era". [Online]. Available: http://surl.li/qmmgf. Accessed on: 12.02.2024.
O. E. Radutnyi, "Shtuchnyi intelekt yak subiekt zlochynu", *Informatsiia i pravo*, №4(23), pp. 106-115, 2017. [Online]. Available: http://surl.li/qmmhp. Accessed on: 12.02.2024. (In Ukranian).
M. Karchevskyi, O. Radutniy, "Artificial intelligence in Ukrainian traditional categories of criminal law", Visnyk Asotsiatsii kryminalnoho prava Ukrainy, №1(19), 2023. [Online]. Available: http://surl.li/qmmkw. Accessed on: 12.02.2024. (In Ukranian).
Kryminalne pravo (Zahalna chastyna): navchalnyi posibnyk / S.A. Shalhunova, O.S. Skok, T.V. Shevchenko, O.I. Sobol, S.M. Shkola, S.A. Rybianets, Yu.V. Voloshyna, A.O. Mariienko, V.A. Yakushkin; za zah. red. k.iu.n., dots. S.A. Shalhunovoi. Kherson: Ailant, 2019. p. 296. [Online]. Available: http://surl.li/qmmnp. Accessed on: 13.02.2024. (In Ukranian).
O. V. Us, "Teoriia ta praktyka kryminalno-pravovoi kvalifikatsii: lektsii". Kharkiv: Pravo, 2018. p. 368. [Online]. Available: http://surl.li/himvj. Accessed on: 13.02.2024. (In Ukranian).
Vidpovidalnist za elektronno-komunikatsiine shakhraistvo: Radi rekomenduvaly pryiniaty zakonoproiekt. [Online]. Available: http://surl.li/qmmsp. Accessed on: 13.02.2024. (In Ukranian).
RICAS - Realtime intelligence crime analytics system. [Online]. Available: http://ricas.org. Accessed on: 13.02.2024.
T.A. Shevchuk, Ya.V. Svystun, "Vykorystannia shtuchnoho intelektu u protydii zlochynnosti", *Visnyk kryminolohichnoi asotsiatsii Ukrainy*, №2(25), pp.128-134, 2021. [Online]. Available: http://surl.li/olzhi. Accessed on: 13.02.2024. (In Ukranian).

Tsyvilnyi protsesualnyi kodeks Ukrainy. [Online]. Available: http://surl.li/qmmzd. Accessed on: 13.02.2024. (In Ukranian).
Zakon Ukrainy «Pro zakhyst personalnykh danykh». [Online]. Available: http://surl.li/jria. Accessed on: 13.02.2024. (In Ukranian).
Proekt Zakonu «Pro zakhyst personalnykh danykh». [Online]. Available: http://surl.li/qmnav. Accessed on: 14.02.2024. (In Ukranian).
Temperature rise is 'locked-in' for the coming decades in the Arctic. [Online]. Available: http://surl.li/qmnka. Accessed on: 14.02.2024.
Vsesvitnii ekonomichnyi forum «Vykorystannia shtuchnoho intelektu dlia Zemli». [Online]. Available: http://surl.li/qmnlr. Accessed on: 14.02.2024. (In Ukranian).
Shtuchnyi intelekt (ShI) na zakhysti klimatu, ekolohii ta bioriznomanittia. [Online]. Available: http://surl.li/qmnoa. Accessed on: 14.02.2024.
N. Miuller, "Shtuchnyi intelekt - nova ekolohichna zahroza?". [Online]. Available: http://surl.li/qmnqj. Accessed on: 14.02.2024. (In Ukranian).
D. Rolnick, and etc., "Tackling Climate Change with Machine Learning". [Online]. Available: http://surl.li/qmnrr. Accessed on: 14.02.2024.
O. Kovalenko, "Prohnozovane ahro. Yak za dopomohoiu mashynnoho navchannia dolaty naslidky zmin klimatu". [Online]. Available: http://surl.li/qmnzn. Accessed on: 14.02.2024. (In Ukranian).
Ukrainskyi hidrometeorolohichnyi instytut. [Online]. Available: http://surl.li/qmoaz. Accessed on: 14.02.2024. (In Ukrainian).
Call for Submissions: Emerging Topics in AI. [Online]. Available: http://surl.li/qmoch. Accessed on: 14.02.2024.
IBM and NASA teamed up to build the GPT of Earth sciences. [Online]. Available: http://surl.li/jtjnh. Accessed on: 14.02.2024.
Do i pislia. Naslidky povnomasshtabnoi viiny dlia ekolohii Ukrainy. Pohliad z suputnyka. [Online]. Available: http://surl.li/mkgmr. Accessed on: 14.02.2024. (In Ukranian).
Zakon Ukrainy «Pro vnesennia zmin do deiakykh zakonodavchykh aktiv Ukrainy shchodo derzhavnoi systemy monitorynhu dovkillia, informatsii pro stan dovkillia (ekolohichnoi informatsii) ta informatsiinoho zabezpechennia upravlinnia u sferi dovkillia» 20 bereznia 2023 roku № 2973-IX. [Online]. Available: http://surl.li/qmoev. Accessed on: 14.02.2024. (In Ukranian).
Henri Kissindzher - Erik Shmidt - Daniel Huttenlokher. ChatGPT provishchaie intelektualnu revoliutsiiu. [Online]. Available: http://surl.li/qmojk. Accessed on: 14.02.2024. (In Ukranian).
D. Makhnenko, "I znovu pro shtuchnyi intelekt. Dopomoha, zahroza chy pusti balachky?". [Online]. Available: http://surl.li/aikch. Accessed on: 14.02.2024. (In Ukranian).
V. V. Kyrychenko, "Sotsialno-psykholohichna paradyhma rozuminnia evoliutsii shtuchnoho intelektu", *Psykholohiia ta sotsialna robota*, v.2(58), pp. 17-24, 2023. [Online]. Available: http://surl.li/qmomd. Accessed on: 14.02.2024. (In Ukranian).
S. P. Derevianko, Yu. V. Prymak, I. M. Yushchenko, "Shtuchnyi intelekt ta emotsiinyi shtuchnyi intelekt yak fenomen suchasnoi kohnityvnoi psykholohii", *Naukovi zapysky Natsionalnoho universytetu «Ostrozka akademiia». Seriia «Psykholohiia»*, №11, pp. 115-119, 2020. [Online]. Available: http://surl.li/qmonl. Accessed on: 14.02.2024. (In Ukranian).
V.I. Liashenko, O. S. Vyshnevskoho, "Tsyfrova modernizatsiia ekonomiky Ukrainy yak mozhlyvist proryvnoho rozvytku: monohrafiia". Kyiv: NAN Ukrainy, In-t ekonomiky prom-ti, p. 252, 2018. [Online]. Available: http://surl.li/wgwf. Accessed on: 14.02.2024. (In Ukranian).

DOI 10.5281/zenodo.10822079
UDC 37.018.43:004-049.5

CHAPTER 20.
SECURITY OF DATA ACCESS IN E-LEARNING SYSTEMS: THREATS AND WAYS TO OVERCOME THEM

Olena HAITAN
Senior Lecturer
National University «Yuri Kondratyuk Poltava Polytechnic»
Department of Computer and Information Technologies and Systems
(Poltava, Ukraine)
olena.haitan@gmail.com
https://orcid.org/0000-0002-7228-9937

Abstract. The widespread use of e-learning systems in both academic and non-academic organizations made it necessary to improve both the overall security level and protection against identity spoofing and cheating. Security is a key issue, as it forms the basis of trust in the online learning results. There are many risks associated with security, such as confidentiality loss, personal data compromising, availability, forgery and destruction of materials and learning outcomes. The paper focus is on the vulnerabilities of learning systems and how to increase data security. The attacks relevant to the learning systems are presented as well. The paper examines the authentication methods in e-learning systems, main benefits and disadvantages of each method, highlights the associated threats, and provides recommendations for selecting a specific method. The paper considers the threats of academic integrity violation and the technical methods used to protect against them. The legal framework for the collection and processing of personal data in learning platforms is analyzed from the perspective of Ukrainian and European Union legislation.

Keywords: authentication, cheating, e-learning, identity-swap, proctoring, security, vulnerabilities.

БЕЗПЕКА ДОСТУПУ ДАНИХ В СИСТЕМАХ ЕЛЕКТРОННОГО НАВЧАННЯ: ЗАГРОЗИ ТА ШЛЯХИ ЇХ ПОДОЛАННЯ

Анотація. Широке використання систем електронного навчання як в академічних, так і в неакадемічних організаціях, призвело до необхідності підвищення як загального рівня безпеки, так і захисту від підміни особи та списування. Питання безпеки є ключовим, оскільки є основою довіри до результатів онлайн навчання. Є багато ризиків, таких як втрата

конфіденційності, компрометація персональних даних, доступність, підробка і знищення матеріалів та результатів навчання. Основна увага у статті зосереджена на вразливостях систем навчання та способах підвищення безпеки даних. Також представлені атаки на системи навчання. Проведено аналіз існуючих методів аутентифікації, які можуть використовуватися у системах електронного навчання. Визначені основні переваги та недоліки, виділені загрози, пов'язані із використанням кожного із методів, сформовані рекомендації щодо вибору конкретного методу. Розглянуто загрози порушення академічної доброчесності та технічні методи захисту від них. Проаналізовано правові основи збору та обробки персональних даних у навчальних платформах з точки зору законодавства України та Європейського Союзу.

Ключові слова: аутентифікація, списування, електронне навчання, підміна особи, прокторінг, безпека, уразливості.

Introduction. Due to the quarantine caused by the spread of COVID-19, the educational institutions worldwide have switched to online or blended learning. E-learning systems have been actively used not only for classes and final student assessment, but also for testing and certifying employees of various organizations. The demand for e-learning systems in both academic and non-academic organizations has led to an increased need for improved security and development of measures to prevent identity spoofing and cheating.

Security is a key issue taking into consideration the rapid increase in the number of cyberattacks starting from 2020. According to IRONSCALES survey, over 80% of institutions globally have faced a rise in email phishing attacks. The APWG Phishing Activity Trends Report showed that 5% of all Ransomware attacks were observed in Education sector among all phishing attacks (fig. 1).

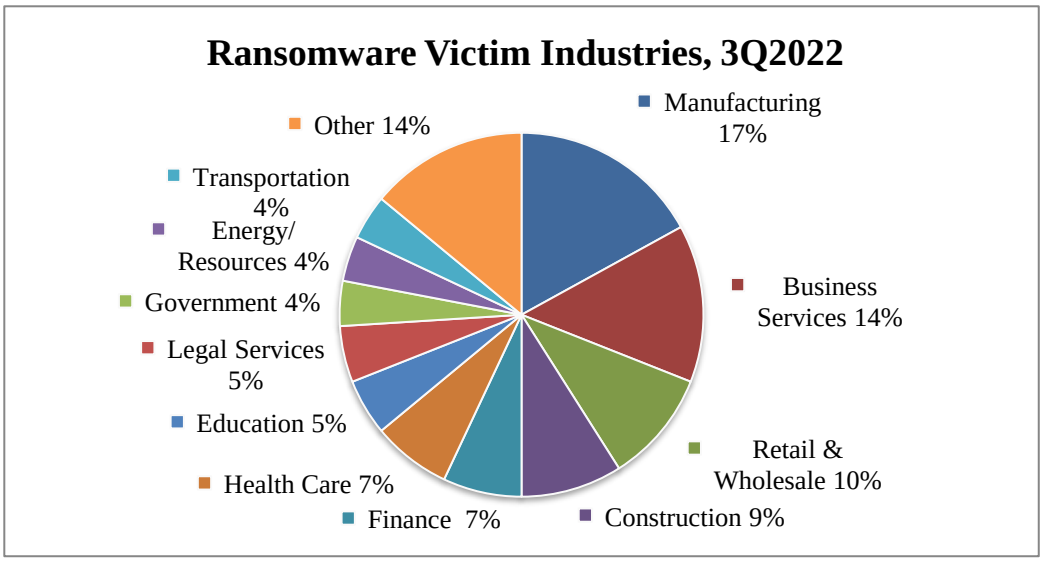


Fig. 1. Distribution of Ransomware attacks among industries

According to the State of Ransomware in Education 2023 report, education providers have experienced a double increase of attacks from 2021 to 2023 (fig. 2).

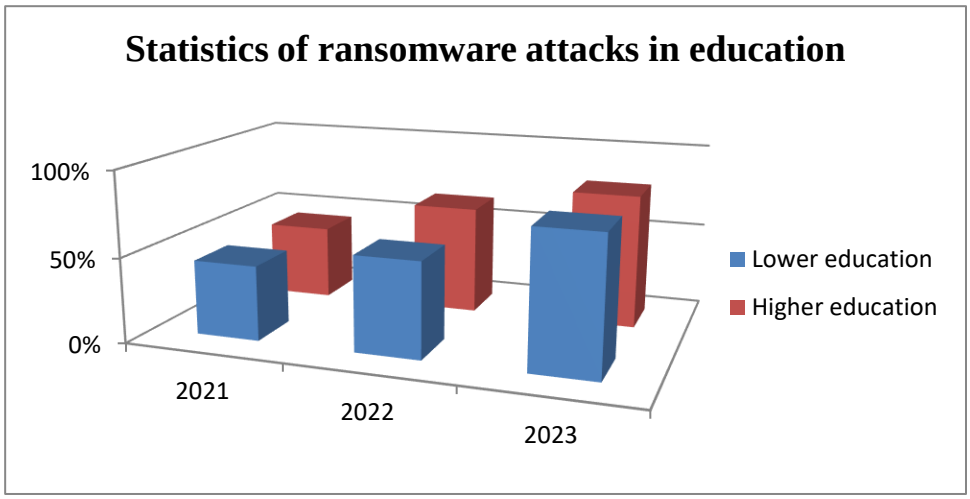


Fig. 2. Statistics of Ransomware attacks in education

However, there has been no increase in recovery costs for education providers, and for higher education, it has decreased from $1.42M to $1M, indicating that the systems are becoming more secure. Analysis of cyberattack statistics in education shows that compromised credentials and exploited vulnerabilities remain the main root causes of the attacks (fig. 3).

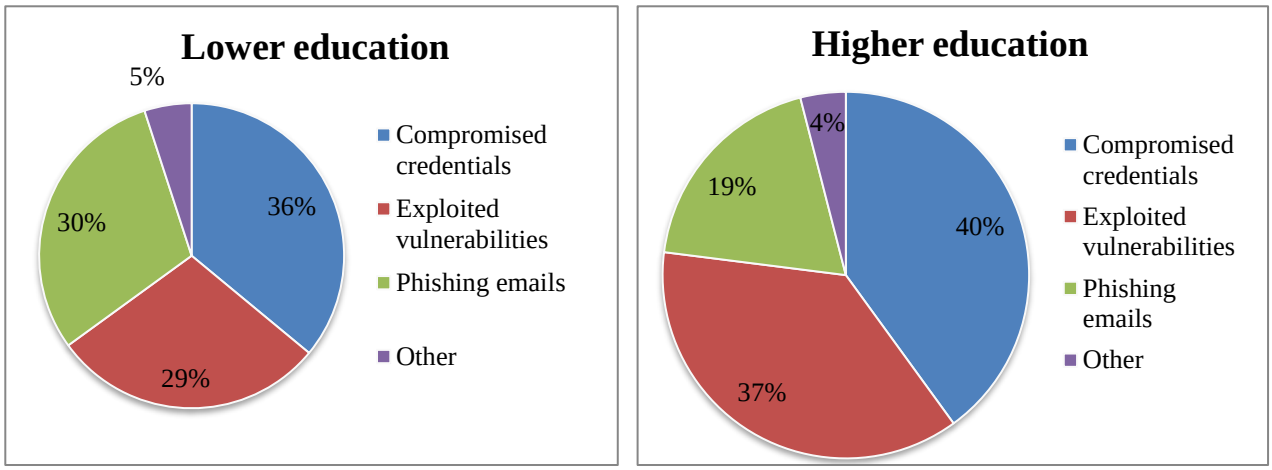


Fig. 3. The root causes of the cyberattacks in education

The problem statement. The main aspects of information security are confidentiality, integrity, and availability. Confidentiality refers to protecting information from unauthorized access, while integrity ensures protection against unauthorized modification of data. Availability, on the other hand, ensures that information is accessible to those who are authorized to access it. The key concepts of the service infrastructure for the security of data control and protection against unauthorized access are identification, authentication and authorization. Luu Q. et al. (*Luu Q. et al., 2020*) emphasize that objectivity and reliability of the e-learning system, in particular online testing, depends on its ability to protect test results from fraud, spontaneous or voluntary interference and identity-swap. Since the online test is conducted in an uncontrolled environment outside the classroom, where institutions do not control student identities, the task of the learning management system is to ensure that the test is taken by the registered student.

Other key aspects of information security are risk management (assessing potential threats and implementing measures to prevent or mitigate their impact), encryption and hashing to protect sensitive information, auditing and monitoring to identify malfunctions or potential threats, and staff awareness and training on information security rules.

The aim of the paper is to consider various issues of information security related to the e-learning systems.

Analysis of recent studies and publications.

Learning systems' security risks. The OWASP Top 10 Vulnerabilities for 2021 ranks Broken Access Control as the most significant web application security risk, followed by Cryptographic Failures in second place and Injection in third place. Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures, Software and Data Integrity Failures, Security Logging and Monitoring Failures, and Server-Side

Request Forgery complete the top ten leaders. The relevance of security risks to the learning systems within the OWASP Top 10 framework is discussed in Table 1.

Table 1. Security risks to the LMS components within the OWASP Top 10

OWASP Top 10	Implementation to LMS	Example
A01:2021 Broken Access Control	Inadequate or incorrect rules for access to courses, materials, or LMS functionality that could lead to unauthorized access or disclosure of confidential information.	Student gets access to assessment results or other student data due to a misconfigured permission settings
A02:2021 Cryptographic Failures	Weak encryption protocols or improper use of cryptographic algorithms within LMS components leading to data breaches or unauthorized access	Storing user passwords in the LMS database using weak encryption or in plain text makes them vulnerable to interception or decryption
A03:2021 Injection	The LMS is vulnerable to attacks such as SQLi and XSS due to a lack of filtering or validation of data input. Injections target database or other components through input fields, API, etc.	SQLi attack injects SQL code into LMS form fields to get access to database with admin privileges and to delete records in it
A04:2021 Insecure Design	Problems in components design lead to vulnerabilities such as hardcoded credentials, lack of required password fields, improper validation mechanisms, attack non-detection, insecure defaults etc.	The hardcoded password of LMS admin account makes it susceptible to brute force attacks
A05:2021 Security Misconfiguration	Poorly configured security settings within LMS servers, databases, or frameworks such as open ports, unencrypted configuration files, default admin passwords	The LMS has open admin access ports or default admin credentials that can be used for unauthorized access
A06:2021 Vulnerable and Outdated Components	Using of outdated versions of frameworks, libraries, plugins and other components within the LMS ecosystem	The LMS uses an outdated version of library that contains known vulnerabilities and can be exploited by attackers
A07:2021 Identification / Authentication Failures	Missing or weak user authentication, insufficient login authentication, improper session implementation	No blocking of multiple attempts increases risk of brute force attacks
A08:2021 Software and Data Integrity Failures	Lack of mechanisms ensuring the software or data the integrity in the LMS, makes it vulnerable to tampering or manipulation	The modification of student grades data, introduction of malicious code, and loss of data due to system failures.
A09:2021 Security Logging and Monitoring Failures	The absence of a security monitoring system, improper configuration and analysis of event logs, and lack of anomaly detection mechanisms	System does not response to security incidents properly: unauthorized access or data leakage remain unnoticed
A10:2021 Server-Side Request Forgery	Requests from the server to external resources can potentially lead to data leakage, DDoS attacks, etc.	The LMS is tricked by an attacker into making requests to internal systems, which can result in unauthorized access or data leakage

To ensure security in the learning system it is also important to find out attack relevant to this type of the software.

Table 2. Attacks relevant to the learning systems

Attack	Attack Description	Preventive Measures	Vulnerable LMS elements	Example of vulnerability
Cross-Site Scripting (XSS)	Injection malicious code into web page generated by the web system	Input validation, output encoding, and CSP headers	Input fields, discussion forums, messaging system	XSS vulnerabilities in LMS messaging allow to send malicious message containing scripts that steal user session tokens
SQL Injection (SQLi)	Injection of malicious SQL into the query through input fields	Parameterized queries, input validation, proper database privilege management	Login form, search fields, enrollment page	SQLi vulnerability in LMS login form allows manipulating database
Cross-Site Request Forgery (CSRF)	Trick authenticated users into executing unwanted actions	Anti-CSRF tokens, SameSite attribute for cookies, and re-authentication for sensitive actions	Forms, buttons, links starting actions	CSRF vulnerability in LMS enrollment system allows automatic enrollment into unauthorized courses
MITM (Man-in-the-Middle) Attacks	Intercept communication between users and LMS to eavesdrop or modify data	HTTPS/TLS encryption, secure communication channels, certificates	Communication channels, login forms, authentication tokens	MITM vulnerability in LMS login process allow interception and manipulation user credentials
Session Hijacking	Steal session token to impersonate legitimate users	Secure session management, HTTPS, and secure cookies	Session management mechanisms, authentication tokens	Session hijacking vulnerability in LMS authentication allows to impersonate legitimate users and access sensitive data
Brute Force Attack	Using automated trial-and-error methods to get user credentials	Strong password policies, attempts blocking, multi-factor authentication	Login forms, password reset mechanisms	Lack of attempts blocking mechanism in the login form allow to perform brute force attacks and get unauthorized access
Data Breaches	Unauthorized access to the LMS sensitive information	Sensitive data encryption, access control, and regular security evaluation	Database, learning materials or learning records	Data breach vulnerability in the LMS database lead to expose sensitive user information
Phishing Attacks	Stealing confidential user information by spoofing or after clicking on	Authentication mechanisms, and anti-phishing tools	Communication channels, login page, notification system	Phishing vulnerability in LMS email notification system allows sending fake notifications to users in order to get their login

Attack	Attack Description	Preventive Measures	Vulnerable LMS elements	Example of vulnerability
	malicious link			credentials
Insufficient Access Controls	Allow unauthorized users to get access to sensitive content or do unauthorized actions	Role-based access control, regular access reviews, and using the principle of least privilege	User roles and permissions, administrative functions	Lack of proper access control allow to the unauthorized access to system management and learning materials
Client-Side Request Forgery (CSRF)	Trick the client-side system into making unauthorized requests	Input validation, server-side validation of user requests, and restrict access to sensitive resources	API endpoints, user input fields, integration points	CRE vulnerability in file uploading allows uploading malicious files to the server or access to restricted resources
Denial of Service (DoS)	Overload LMS with requests, making it unavailable to legitimate users	Rate limiting, web application firewalls, and anti-DDoS services	Server, network infrastructure, authentication system	DoS vulnerability in LMS login page allows flooding the server with user requests, and it becomes unresponsive
HTTP Response Splitting	Inject malicious HTTP headers into HTTP responses to manipulate response	Validate and sanitize user input, encode output properly, and configure server securely	HTTP response, input fields, server configurations	HTTP response splitting in the URL redirection allows to inject malicious URL into HTTP response, leading to phishing or redirection attacks
Server-Side Request Forgery (SSRF)	Trick server into making unauthorized requests to internal / external resources	Validate / sanitize user input, restrict access to sensitive content, and server-side validation of user requests	API endpoints, file upload/ download functionality, integration points	SSRF vulnerability in the course material download allow access to restricted files or internal resources by manipulating the server's requests
Remote Code Execution (RCE)	Attempt to execute malicious code on a remote system by bypassing security restrictions	Strict access control over code execution, security updates, network filters and firewalls	Files upload feature, dynamic pages, and custom code execution mechanisms	Uploading of user-generated content, such as course files, can be the source of vulnerability that allows malicious code execution on server

Odeh N. & Hijazi Sh. (*Odeh N., Hijazi Sh., 2023*) present an overview of common web vulnerabilities, including SQLi, XSS, RCE, and fingerprinting of backend technologies and discuss ways to prevent them. The paper explains the functionality of each vulnerability and outlines using of detection methods to identify them. Additionally, it proposes preventive measures to mitigate each vulnerability type. Bhatia M. & Maitra J.K. (*Bhatia M., Maitra J.K, 2018*) discuss the results of Open-

Source E-Learning Platforms scanning by Vulnerability Scanners Netsparker and Acunetix (fig. 4).

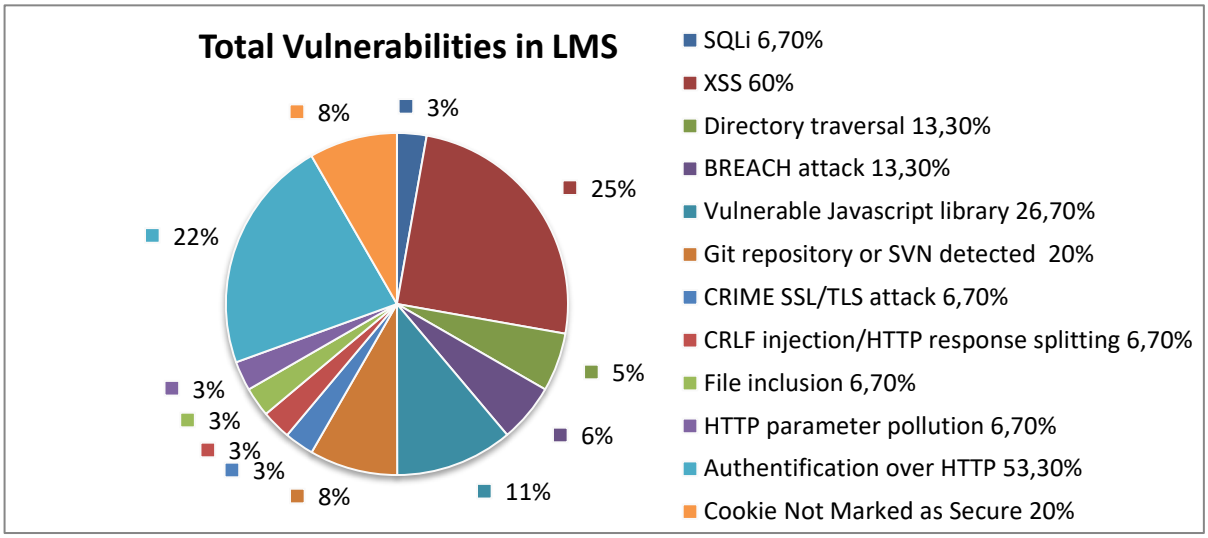


Fig. 4. Classification of vulnerabilities in the learning management systems

The top Vulnerabilities found by both scanners over all platforms are XSS (60%), Authentification over HTTP (53,3%), vulnerable Javascript libraries (26,7%).

Djeki E. et al. (*Djeki E. et al., 2021*) examined vulnerabilities and cyberattacks and their impact on digital learning platforms, as well management and user operational risks caused by human errors and ignorance. The paper introduces a comparative study on the vulnerabilities of the most used Learning Management Systems using the classification of the web application vulnerabilities presented by the OWASP and CWE. The research showed that Moodle is the most vulnerable to attacks LMS, and Blackboard is the most secure one. Vulnerabilities of Moodle and ways to eliminate them are considered in papers of Al-azaiza R. (*Al-azaiza R., 2016*), Barhoom T.S. & Azaiza R.J. (*Barhoom T.S., Azaiza R.J., 2016*), Yousif A. & Badawi M. (*Yousif A., Badawi M., 2020*), Yaseen K.A.Y. (*Yaseen K.A.Y., 2023*), Elmaghrabi A.Y. & Eljack, S.M. (*Elmaghrabi A.Y., Eljack, S.M., 2019*), Ally S. (*Ally S., 2022*) discuss security of Quiz module in Moodle. It is noted that Moodle is vulnerable to security threats due to its open-source nature. This problem can be solved by the development and use of security plugins, as well as careful configuration of security settings. To get maximum benefits of using Moodle, Ally S. recommends regularly updating to the latest stable version and using of security patches, registering officially with Moodle.org, using proper computing infrastructure including auto-update systems, rootkit detectors, and spam cleaners, enabling only necessary features and services for online exams, setting centralized institutional security configurations, configuring default settings, reviewing source codes, and setting file and user permissions. Akacha S.A.-L. & Awad A.I. (*Akacha, S.A.-L. Awad, A.I., 2023*) provide the comparative analysis of the vulnerabilities in Moodle, Chamilo, and Ilias LMS using Common

Vulnerabilities and Exposures (CVE) database, available online, and their own experimental data.

Pillajo-Garcia P. & Avila-Pesantez D. (*Pillajo-Garcia P., Avila-Pesantez D., 2023*) performed a systematic literature review on cybersecurity in three learning platforms: Moodle, Microsoft Teams, and Blackboard. A detailed analysis of use of the videoconferencing systems (Google Meet, Microsoft Teams, and Zoom) during online classes, including security issues, is discussed by Haitan O. (*Haitan O., 2022*).

Fonar L.S., Konovalov O.S., Filippov E.G. (*Fonar L.S., Konovalov O.S., Filippov E.G., 2022*) studied information security threats in educational systems. They note that attackers, both external and internal, aim at such goals when implementing an attack:

– Exceeding privileges;

– Unauthorized access to resources;

– Control over the course;

– Access to the university internal system;

– Intellectual property theft;

– Assessment materials theft;

– Unauthorized access to personal data;

– Disclosure of personal data;

– Making changes to the database of academic information with grades and modules;

– Unauthorized access to official information of the educational institution;

– Violation of integrity or destruction of educational materials;

– Violation of integrity or destruction of data related to the educational process;

– Violation of users' accessibility to materials of educational courses.

Approaches to the security model, based on the LMS architecture. Bhatia M. & Maitra J. K. (*Bhatia M., Maitra J.K., 2018*) describe two approaches to organizing the security model in LMS. The most common one is the hierarchical approach, where the system administrator controls security from the top of the tree. In distributed architecture each element may support individual security model. These security models may have different security logics but they must interact between each other. The advantages of this approach are scalability, possibility of the segmented system modification, and flexibility in choosing security mechanisms.

Khan M., Naz T., & Mahmood Kh. (*Khan M., Naz T., Mahmood Kh., 2019*) propose the development of secure distributed databases in LMS using the Blockchain method (fig. 5). They emphasize that the Blockchain method offers several advantages in terms of cybersecurity. First, Blockchain provides a reliable method for verifying lost or reissued data, as well as for global authentication, ensuring data protection and user privacy. Secondly, the use of cryptographic methods

in Blockchain, such as hashing and the calculation of transaction hashes using the Merkle tree algorithm, ensures a high level of data integrity and system decentralization, making it impossible to manipulate records in blocks. As a result, the LMS is more resistant to cyberattacks and information tampering. Using of Blockchain technology for recording of students' learning trajectory, verification of student certificates, and sharing of learning resources is presented in short paper of Sun H., Wang X., and Wang X. (*Sun H., Wang X., Wang X., 2018*).

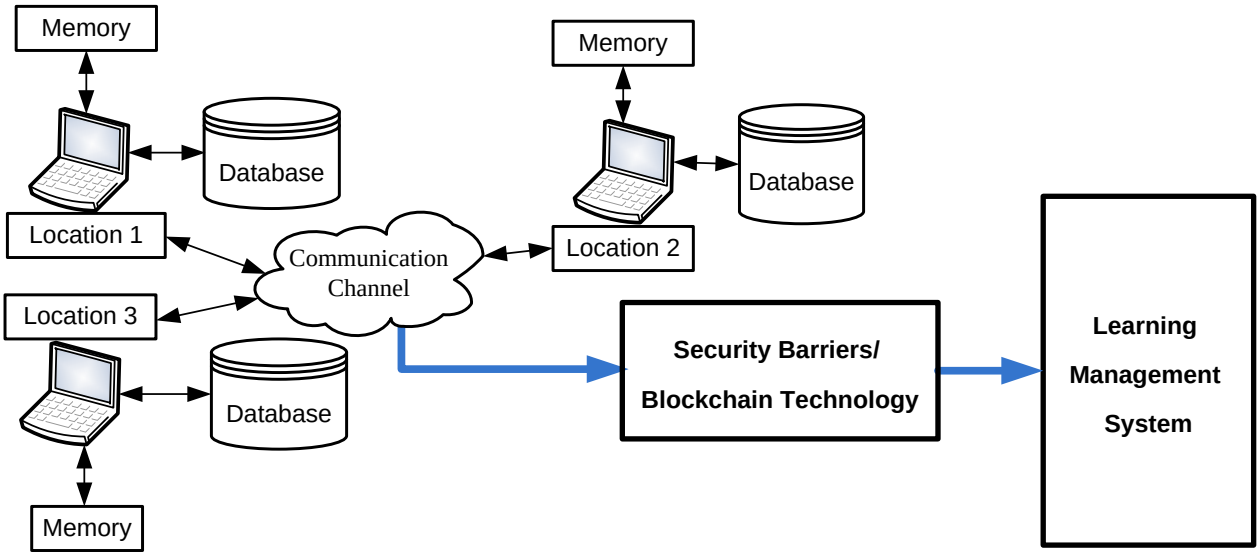


Fig. 5. Architecture of LMS with Blockchain technology

Huk et al. (*Huk O., Loza V., Voloshko S., Kurchanov V., 2020*) investigated the use of VPNs to provide secure access to distance learning systems. The study focused on creating a secure channel between a corporate network segment and an individual user who connects to corporate resources from a home computer during training:

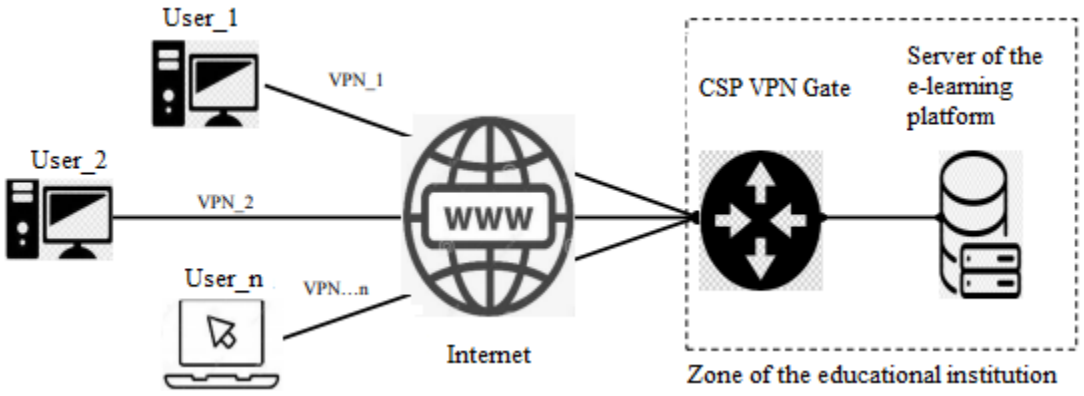


Fig. 6. Organization of secure access to distance learning systems using of VPN

Methods of access control security ensuring in the learning systems

General characteristics of the identification and authentication methods. E-learning systems are perceived as secure only if the student is successfully identified and authenticated.

Identification is a procedure of determining the identity of a registered user, the identifier of teacher or student that uniquely identifies this subject in the information system. Identification by login/ID is carried out by entering and recognizing an existing login/ID as assigned to a specific participant of the educational process. Biometric identification consists in identifying a person by obtaining an element of his biometric data (for example, a photo) and comparing it with the biometric data of several other persons stored in a database.

Authentication is checking of authenticity to prove the identity of a registered user, for example, by comparing the entered password with the password stored in the database. Biometric authentication compares a person's characteristic data with his/her biometric data to determine similarity. Student authentication is recognized as one of the biggest challenges in online education. Students must be strongly authenticated before they can access sensitive content such as tests, assignments, or personal notes.

The general classification of authentication methods is shown in fig. 7.

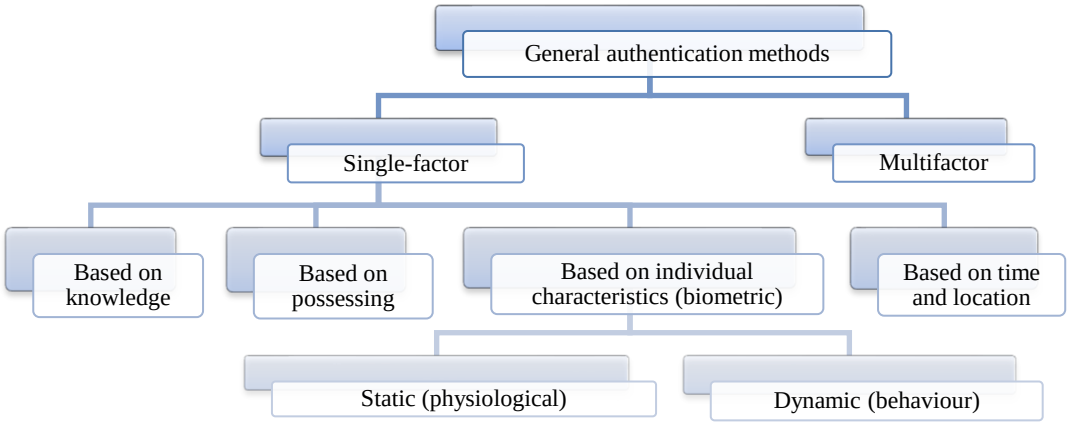


Fig. 7. General classification of authentication methods

To prove the identity of a registered user, three categories of factors are traditionally used: knowledge-based (password, PIN, graphical pattern, etc.), ownership-based (smart card, USB key, hardware token, etc.) or biometric properties (face, fingerprints, etc.). Salameh N. & Shukur Z. (*Salameh N., Shukur Z., 2015*) distinguish four main groups of e-authentication are: "knowledge-based", "possessed-based", "biometric" and "other" (based on date and time). To this list, Okada A. et al. (*Okada A. et al., 2019*) add the tools offered by the TeSLA (adaptive trust-based e-assessment system for learning), in particular anti-plagiarism software and forensic text analysis.

The characteristics of authentication methods for e-learning systems by category are

considered in many research works, in particular:

1. Knowledge-based systems are based on information stored by the user. The main advantages are ease of use and low cost, the main disadvantage is low security level, since knowledge-based tools are vulnerable to attacks and impersonation.

2. Systems based on biometric features are based on the unique static (physiological) and dynamic (behavioral) person features. Physiological properties are given to a person from birth on the basis of genetic data, are inherent in a person throughout life and do not change significantly with time.

Static properties include fingerprints, facial geometry (2D or 3D), iris, and retina. Behavioral properties characterize the dynamics and style of performing a certain act. Dynamic properties include voice, stroke, signature, keyboard handwriting, etc. The main advantages are the identification accuracy and constant feature presence; the main disadvantages are the difficulty in implementing of technological solutions and the high cost of scanners.

3. Systems based on ownership use private devices owned by the user. The main advantage is ease of use; the main disadvantage is low security level, since devices can be lost, stolen or forged. This authentication type is the least used in e-learning systems, as students can transfer their authentication devices to other individuals for taking exams.

4. Additional location and time based restrictions improve authentication strength and include IP or MAC address restrictions, test pass timestamps, etc. This tool can be used as an additional tool for authentication.

Authentication methods by category are presented in the table 3.

Table 3. Authentication methods by category

Knowledge-based	**Possession-based**	**Based on individual characteristics (biometric)**	**Integrated methods**
Unique identifier (ID, QR-code), PIN, Password, Passcode, Graphical password, lock pattern Security question	Smart card / Memory card Physical identification key Token (hardware token, USB key, cryptographic token) Smartphone E-mail	Face Fingerprints Voice, speech Eye iris, eye retina Palm veins Keyboard handwriting	FIDO TeSLA Bank ID

Since the responsibility for the safety and protection against personal data compromise lies with the operator of such data, other option is to use external resources for authentication. Thus, Lee Aeri, Han Jin-young (*Lee Aeri, Han Jin-young, 2020*) propose to use in e-learning platforms systems Fast IDentity Online (FIDO), developed by FIDO Alliance. FIDO is an authentication system that

defines an open, scalable set of mechanisms based on biometric information and various authentication methods without need to remember a password. FIDO authentication is a set of security technology specifications designed to authenticate a user's identity in an online environment in a comfortable and non-dangerous way using biometric authentication. According to the authors, FIDO authentication is the next generation authentication system that will replace the password, but no practical application in e-learning systems is given.

General characteristics of authentication methods in e-learning systems is presented in tab. 4 – 10.

Table 4. General characteristics of authentication methods in e-learning systems

Method	Description	Benefits	Disadvantages	Threats	Link
Password / ID / secret question	Based on information stored by the user	Usual method for users Low cost No additional devices	Low security level Need for remembering / storage	Compromise / attacks on the system Identity-swap Loss / theft	[48] [59]
Device-based authen-tication	Use of devices registered in system or tokens stored on hardware storage	Ease of use for users Multi-service	Need for additional reading equipment Need for client drivers Low security level Need to carry device	Identity-swap Loss / theft / forgery / emulation Compromise using principle "one key to all"	[39]
Biometric authen-tication	Based on the unique human features	Uniqueness of the features Possibility of authentication in real time (keyboard handwriting, proctoring). Ease of use for the user Features are always available	High price / Need for additional reading equipment Need for integration with learning platform Influence of psychological state / lighting / accessories Possibility of change over time / due to surgery / scars Recognition accuracy Depend on technologies Implementation complexity Requirements of regulators	Compromise Forgery/ emulation for some biometric methods Users' reluctance to provide personal data Errors of the first and second kind	[23] [45] [64] [67] tab. 5-9
Multi-factor authen-tication	Combination of unbound methods	Increasing the security level due to method combination	Inconvenient interface Difficulty in implementation High cost		[25]
Use of external authen-tication resources	FIDO, Bank ID, Google account etc.	No need to store personal data	Need for integration with the learning platform Need for client drivers	Dependence on security/ accuracy of external resource	[40] [47]

Table 5. Characteristics of fingerprint authentication

Description	Benefits	Disadvantages	Threats	Link
Papillary pattern of fingertips is scanned using a special scanner, converted into a digital code and compared with patterns in DB	High accuracy The most widespread method of bioidentification Integral part of a person, feature does not change over time	Difficulty of implementation Need for additional reading equipment Low identification accuracy for damaged / dirty fingers	Compromise Identity-swap when using a film with printed fingerprint	[23] [25] [31] [35]

Table 6. Characteristics of face recognition authentication

Description	Benefits	Disadvantages	Threats	Link
Frontal face photo is made, characteristic features are highlighted, converted into a digital code and compared with templates in DB	No need for additional equipment if there is a built-in camera An integral part of a person	Influence of psychological state / lighting / accessories Change over time / due to surgery / scars Unreliability of 2D / Cost of 3D face recognition	Identity-swap using a photo (video) instead of a student Deepfakes	[21] [23] [57]

Table 7. Characteristics of voice and speech authentication

Description	Benefits	Disadvantages	Threats	Link
Passphrases (more than 5seconds) or fragments of spontaneous speech are turned into a voice template and compared with templates in DB	Possibility of remote identification Increased reliability with a combination of voice identification and voice password recognition An integral part of a person	Low accuracy Change over time Significant influence of psychological / health state Depend on quality of voice signal transmission channel Negative influence of ambient noise Depend on used technology Impossibility of use by mute people and people with serious speech problems	Emulation using special software	[51]

Table 8. Characteristics of eye iris and eye retina authentication

Description	Benefits	Disadvantages	Threats / Link
Iris is scanned, converted into a digital code and compared with templates in DB	High accuracy of identification An integral part of a person, feature does not change over time	Absence of reliable methods for remote identification Need for additional equipment / High cost Use of complex technological solutions Discomfort from the thought of a harmful effect on vision	At the moment, it is not used in e-learning due to equipment cost, but paper [55] considers iris authentication on a mobile exam using a phone camera

Eye retina is scanned using low-intensity infrared light, converted into a digital code and compared with templates in DB	High accuracy of identification An integral part of a person, feature does not change over time	Absence of reliable methods for remote identification Need for additional equipment / High cost Use of complex technological solutions Discomfort from the thought of a harmful effect on vision	At the moment, it is not used in e-learning due to equipment cost

Table 9. Characteristics of eye palm veins and palm print authentication

Description	Benefits	Disadvantages	Threats	Link
Palm is scanned in multi-spectral infrared light. Resulting pattern of blood vessels is converted into a digital code and compared with templates in DB	Unambiguous identification An integral part of a person, feature does not change over time	Need for additional equipment / High cost Distortion of information in case of arthritis and other diseases of the circulatory system	At the moment, it is not used in e-learning due to equipment cost	
Palm is scanned, characteristic features are extracted, converted into a digital code and compared with templates in DB	Integral part of person Ease of template getting No influence of temperature, humidity, pollution Low image requirements Small template size	Need for additional equipment Distortion of information in case of arthritis, bruises, bone damage and other diseases Low recognition accuracy	Errors of the first and second kind	[22]

Table 10. Characteristics of keyboard handwriting authentication

Description	Benefits	Disadvantages	Threats	Link
Text fragment is entered, for which parameter (time intervals between button presses etc.) are measured, entered into a matrix and compared with templates in DB	No need for additional equipment Effective for real time authentication Effective for additional authentication	Significant impact of psychological/health status Ability to change over time More time required for identification Significant amount of data is required for identification	Errors of the first and second kind	[29] [30] [37] [57] [61]

General overview of authentication methods in e-learning systems is given by Luu Q. et al (*Luu Q., Nguyen D., Pham H., Huynh-Tuong N, 2020*).

Authentication subsystems in the e-learning system are vulnerable to various threats depending on the method used (tab. 11).

Table 11. Threats and vulnerabilities of authentication methods in e-learning

Knowledge	Using device	Biometric methods

Forgetting	Possibility of loss / theft	High cost
Brute-force attack	High cost	Need for additional equipment
Dictionary attack	Inconvenience of using	Impact of lighting and accessories
Software keyloggers	Need for reading equipment	Surgery and scars
MITM attack	Need to install client drivers	Influence of psychological state
Replay attack	MITM attack	Recognition accuracy
Screen capture	Forgery / emulation	Forgery / emulation
Spying on the password over the shoulder		Replay attack

The most common threats in face and fingerprint recognition are:

1. Deepfake is artificial intelligence-based synthesis of a person image by combining and overlaying additional images on real image or video. A case was recorded when a well-known pornographic actress passed safety tests at an enterprise.

2. An attempt of physical face-swap. A case was recorded when a test participant printed someone else's photo on A4 sheet, cut out eyes and used the photo as a mask.

3. Attachment of a fingerprint printed copy to the scanner. In this case, the falsification is possible when using an optical reader and it is impossible when using a fingerprint multispectral reader.

Password or token authentication checks for 100% match with the parameter in the database, while bio-authentication extracts key points or key characteristics that are compared with the information stored in the database using the mathematical apparatus of fuzzy search or certain metrics.

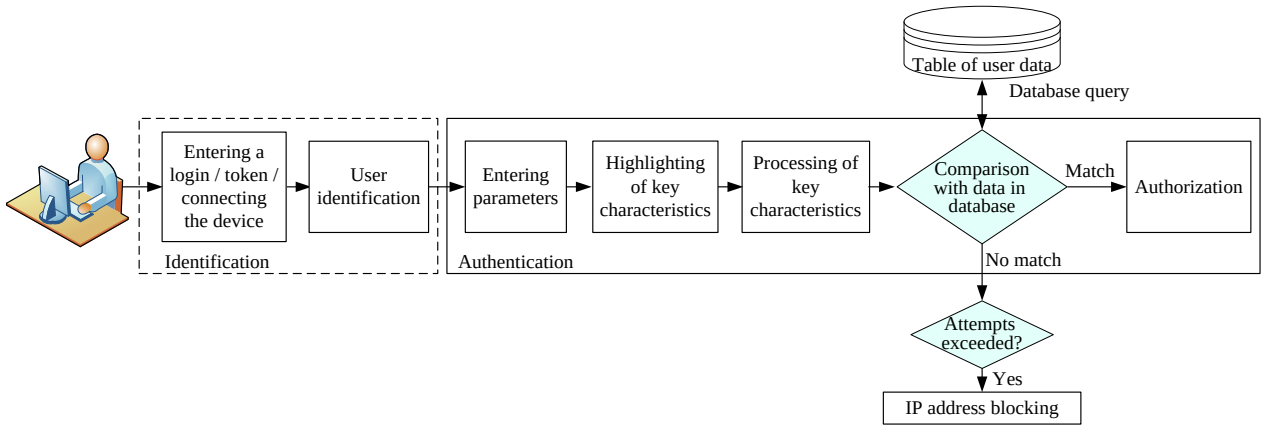


Fig. 8. Sequence of actions during user authorization in the system

The matching threshold must be set by looking for a balance between errors of the first (false rejection of the true user) and the second (recognition of the false user) kind. Timirgaleeva R.R. et al. (*Timirgaleeva R.R., Grishin I.Yu., Mironov M.V., 2019*) propose to use the mathematical apparatus of fuzzy sets to reduce the uncertainty of the input data. In order to identify the user image, as a metric

to determine the relationship between the quantitative characteristics of the user's statistical characteristics and the reference ones, the Euclidean distance and the quadratic fuzziness index between the vectors of the membership functions of the input sets and the saved profile characteristics are chosen. The use of the Euclidean distance between the characteristics determined on the basis of measurements of the new user's keyboard handwriting and the profiles of all users in the database as a metric is also considered by Zamfiroiu A. et al. (*Zamfiroiu A., Constantinescu D., Zurini M., Toma C., 2020*). To identify the user, it is enough to determine the minimum value in the set of Euclidean distances.

Among biometric methods, the highest false acceptance rate (FAR) and false rejection rate (FRR) are observed in 2D face recognition (FAR – 0.1%, FRR – 2.5%). At the same time, the probability of falsification depends not only on the type of biometric feature, but also on the technology used for its reading. In particular, in long-range scanners built into laptops or connected to a computer via USB, only a small narrow part of the fingerprint is scanned at the same time, as a result fingerprint capture is complicated and a higher number of false access refusals (FRR) is observed compared to a full-contact scanner which immediately captures the entire surface applied to the scanner. But at the same time, the smaller sensor size of a long-range scanner reduces its cost, which increases its use as a built-in authentication tool in electronic devices and applications, and in particular in e-learning systems.

One of the main threats when using biometric methods is their compromise. Biometric identification is based on the fact that biometric features do not change or change only slightly during a person's lifetime, so a compromised feature cannot be replaced as a stolen password. Therefore, it is necessary to take additional measures to protect biometric data. Among the basic principles of biometric data protection, one can highlight the transformation of biometric characteristics and biometric cryptosystems.

The transformation of biometric characteristics is usually based on individual user characteristics. Using the irreversible transformation function for the original template results in a protected template that is stored in the database. The authentication system applies the same transformation function to the request and checks matching for the transformed sample.

Biometric cryptosystems store only part of the information obtained from the biometric template – this part is called a secure sketch. Although it is not sufficient to restore the original template, it contains the necessary amount of data to restore the template in the presence of another biometric sample similar to the one obtained during registration.

Identification, authentication and authorization in e-learning systems. The learning platforms continue using password methods as their primary authentication tool. The most common

biometric authentication methods used in such systems, taking into account the cost and the possibility of using the built-in functions of devices (camera and a fingerprint scanner), are face and fingerprint recognition.

Keyboard handwriting is an effective method of real-time hidden authentication; it is most often used as a method of additional authentication in combination with other tools, for example, Asha S. & Chellappan C. (*Asha S., Chellappan C., 2008*) proposed to use a combination of fingerprints and mouse dynamics.

Standard one-factor authentication cannot provide absolute security during user authorizing in an e-learning system. Therefore, to increase the reliability of authentication when using non-unique biometric characteristics, multi-factor authentication is used, which includes recognition by several unrelated parameters at once. Okada A., etc. claim that an electronic authentication system that combines various tools is more efficient and users perceive it as more reliable. The authors studied the attitudes and experiences of students who used an authentication system known as Adaptive Trust-Based E-Assessment System for Learning (TeSLA). In general, the more factors included in an authentication system, the more secure it is. According to Microsoft, multi-factor authentication can prevent 99.9% of cyberattacks. Levels of protection in e-learning systems using single- and multi-level authentication are given in tab. 12.

Table 12. Levels of protection in e-learning systems using single- and multi-level authentication

Authentication levels		
Single-factor authentication (SFA)	**Two-factor authentication (2FA)**	**Three-factor authentication (MFA)**
Password (very low) Token (very low) Biometrics (low)	Password + biometrics (medium) Password + real-time authentication (high) Biometrics + real-time authentication (very high)	Password + biometrics + real-time authentication (extremely high)

When using two-factor authentication, a combination of password and biometrics is preferred. For example, since the error probability in palm geometry recognizing is about 0.1%, Al-Saleem S.M. & Ullah H. (*Al-Saleem S.M. & Ullah H., 2014*) propose a combination of a palm print and a standard login/password combination.

Ullah A. et al. (*Ullah A., Xiao H., Lilley M., Barker T., 2012*) propose to use test questions to authenticate students in online exams as part of the Student Profile Based Authentication Framework (PBAF). It should be noted that secret questions should not be used as a single mechanism for authentication or resetting passwords and are not recognized as an acceptable authentication factor

according to NIST SP 800-63 because the answer can be guessed or known. However, they can provide an additional security level when combined with other methods. In particular, Ullah A. propose the use of test questions that are randomly selected from the student profile, together with the user ID and password.

Beaudin Sh. (*Beaudin Sh., 2016*) claims that the "one for all" authentication approach is not suitable for all types of e-learning and that the levels of authentication should differ in strength depending on the activity performed in the e-learning system. As a result of the study, it was determined that there is a certain set of activities in the e-learning system, which, according to the participants in the educational process, have a high risk of impersonation fraud and require a medium or high level of authentication to reduce the threat. For better protection of an e-learning system at the activity level, it is required an authentication method different from one-factor authentication that is used to authenticate users at the system level. In particular, the final e-assessment requires more secure authentication method that includes at least biometric authentication and/or real-time authentication.

AbuMansour H.Y. (*AbuMansour H.Y., 2017*), investigating security of the question bank, which is considered the basis of online exams, proposed the introduction of authorized person fingerprint authentication technology as a nested internal information security layer for accessing the question bank. According to the authors, this mechanism can prevent unauthorized users from being given dangerous access to the question bank in case if authorized access with high privileges is left unobserved or in case of a successful attack on the first security level (password/username).

Authorization tool determines whether a verified person has access to certain resources: information, files, and databases.

Let's consider some methods of reducing threats related to authorization:

1. By default, access to resources, including educational materials, should be prohibited, except of access to public resources. Access to resources should be given only to the security engine that checks the appropriate rights. It should be noted that providing direct access to a resource is a violation of the Security through obscurity principle, which is used in various fields of human activity.

2. Automatic block of an IP address after a certain number of unsuccessful attempts to protect against brute force attacks. Such a mechanism helps to stop automated scripts that try to hack the site by selecting various combinations of login and password or by enumerating the contents of directories.

3. Automatic session closing after browser closing or setting this parameter. Experience shows that while using e-learning systems in public places, in particular in the classrooms of an educational institution, teachers and students often forget to log out of an account that provides access to their

account to other people. When using a computer at home, the automatic closing of the session, on the contrary, can cause inconvenience.

4. Automatic session closing after certain time of inactivity / certain time of work (setting the Expires cookie parameter).

5. Captcha does not allows automation of requests for selecting parameters, but the tool may be inconvenient for students or teachers.

To preserve teachers' copyrights to educational materials, it is necessary to provide additional protection options, in particular, prohibition for copying, printing, caching, etc.

Perception of students from different social groups of electronic authentication. A significant problem with any biometric methods is the initial collection of reliable data. People don't want to hand them over, because they do not see any particular benefit for themselves or they are afraid that their personal data can be compromised or misused to their detriment.

Okada et al. (*Okada A., Whitelock D., Holmes W., Edwards Ch., 2019*) conducted a survey among different age groups, social categories and people of different sexes regarding their consent to provide their personal data for electronic authentication and made conclusion that, in general, men are more willing to provide their personal data than women, about half of the respondents agree to provide all necessary personal data. These conclusions are confirmed by other studies, e.g. by Laamanen M. et al. (*Laamanen M., Ladonlahti T., Uotinen S., et al, 2021*). According to these researchers, the risk of confidentiality loss has a stronger effect on the intention to share information for women, while the received benefit has a stronger effect on the consent to share confidential information for men.

While many younger students share their personal data in social media, their attitudes towards security differ in the context of e-assessment as they are more concerned about data privacy and security, while older participants that have limited experience with online assessment are, on average, more willing to trust online assessment e-authentication tools.

Laamanen M. et al., examining views of the students with special educational needs on electronic authentication, made the conclusion that e-authentication is highly acceptable among such students. The vast majority of participants were willing to provide at least one type, and some respondents even all types of personal data. Positive view of students with special needs on e-authentication differs significantly from the conclusions of researchers that analyzed views of students in Open University UK's Institute of Educational Technology, including students with special educational needs. According to these researchers, although e-authentication potentially makes assessment easier for students with special educational needs, they had "average various concerns and relatively negative attitude to e-authentication due to their lack of confidence and

concerns on their limitations".

When comparing the disability type, it was noted that students with visual impairments considered keyboard dynamics less acceptable, probably these students were afraid that the system would not recognize them if, for example, they use an alternative keyboard. Ironically, students with hearing problems were more willing to share recordings of their voices than videos of their faces. Especially for such students, the paper considers the possibility of authentication by voice.

Data encryption. Data encryption plays a crucial role in ensuring data security in e-learning systems and protecting data from being intercepted, modified, or stolen by hackers or malicious actors.

Briliyant O.C. & Baihaqi A. (*Briliyant O.C., Baihaqi A., 2017*) suggest a design for an e-learning system that integrates digital signature and encryption to enhance security within the application. The proposed encryption mechanism uses AES 128-bit, recognized as secure and unaffected by attacks. Additionally, digital signature and hash functions with SHA 256-bit and RSA 2048-bit algorithms are used to ensure integrity, authentication, and non-repudiation.

The example of encryption in e-learning systems is the use of SSL or TLS protocols to encrypt data transmitted between a student's device and the e-learning platform. This encryption ensures that sensitive information such as login credentials, personal details, and academic records are securely transmitted and protected from unauthorized access. For example, Moodle uses the MNet Protocol for secure communication between Moodle instances through RPC calls. The MNet Protocol involves signing and encrypting requests and responses using XML-RPC, XML-SIG, and XML-ENC. It employs public key cryptography, RC4 encryption with a 128-bit key, RSA for signature, and SHA-1 for digest. The protocol also uses 1024-bit RSA key generation and self-signed certificates. Blackboard implements TLS for secure communication between clients and servers.

Encryption of stored data within the e-learning system databases using algorithms like AES provides information safeguarding at rest.

Moodle enhances security by encryption of the stored user passwords within the database using hashing algorithms bcrypt since Moodle 2.5 and adding a unique salt for each individual user (Moodle used MD5 until Moodle 2.5).

Therefore, Moodle does not provide user data encryption at rest, but it does provide mechanisms for secure communication and password storage.

Exact algorithms for user data encryption in Blackboard are not detailed in the provided search results, but compliance with various security standards and frameworks, such as ISO 27001/27017/27018, GDPR, FERPA, California Consumer Protection Act confirm of using of cryptographic techniques to protect user data.

According to the Canvas website, Canvas, an open-source cloud-based LMS by Instructure, uses military-grade data encryption for data in database in transit and at rest. The military-grade data encryption refers to use of robust and highly secure encryption algorithm AES-256. Canvas uses the AWS Key Management Service (KMS) to protect data, which allows users to create and manage cryptographic keys for encrypting data. SageMaker Canvas, a machine learning service provided by AWS, also provides several options for encrypting data, including encrypting data stored in Amazon S3 to protect data at rest.

Additionally, end-to-end encryption can be implemented in communication tools within the e-learning platform to secure interactions between students and instructors during live sessions. These encryption methods help maintain the confidentiality and integrity of data in e-learning environments, enhancing overall security for users.

Chatterjee et al. (*Chatterjee P, Bose R., Banerjee S., Roy S, 2023*) propose using a hybrid cryptography algorithm for a cloud-based LMS. They utilize symmetric cryptography algorithms such as AES, Blowfish, RC6, and BRA for data block-wise security. To ensure key information security, they implement a three-bit LSB steganography technique to obtain a 128-bit Symmetric Key for the aforementioned algorithms.

Online exam security control in e-learning systems. To ensure the security of data transmission, the HTTPS protocol is used, which supports an encrypted connection and provides tools for exchanging authentication information or credentials without being easily intercepted. This method will protect against sniffer attacks and MITM attacks, but will not provide protection against face-swapping when someone tries to take an exam instead of a real student in case the client signs with the original user's certificate.

Rao N.S.S., et al. (*Rao N.S.S. et al., 2011*) proposed to use an advanced online exam security control system (SeCOnE), based on group cryptography in combination with electronic monitoring to reduce the level of fraud during online exams. In this system, all users associated with the exam belong to one of two groups: administration and students, who are given temporary identifiers. Neither they nor the other members of the group know the identity of the second member of the group. In addition, the group member does not know his temporary identifier, since it is given in encrypted form and is protected by the public key of the verifier. The security of the exam is controlled through out-of-group communication based on Public Key Infrastructure (PKI) and in-group communication using symmetric Diffie-Hellman keys and temporary identification. To protect against student cheating, a webcam and e-monitoring are used.

Huszti and Petho (*Huszti A., Petho A., 2010*) described a cryptographic scheme that provides "security requirements, such that authenticity, anonymity, secrecy, robustness, correctness without

the existence of a Trusted Third Party" through use of cryptographic primitives. Pseudonyms are used to identify students. The student generates a secret key at the training beginning, and for each exam a new pseudonym is generated, derived from this original master key, which is kept secret. With a delayed release solution no one can associate a pseudonym with a student before certain time. The use of such a scheme will increase the objectivity of knowledge testing, since neither teacher nor examining body knows the real student during the exam. The management staff only owns the encrypted answers, so they cannot change the students' answers.

Note that in addition to student authentication, teacher (proctor) authentication plays an important role in e-learning systems, since the teacher has access to many aspects of the exam, including student registration data, assignment/test data, current and final grades. If unauthorized access is obtained, this data can be compromised. Therefore, data security is crucial for both the teacher and the student.

Most of the threats associated with the identification methods are attempts to get access to the system without the user knowledge. At the same time, one of the key problems associated with the use of e-learning platforms is the identification of the student. The main danger of online exams is identity-swap. There are two types of substitution fraud. At direct substitution, another person tries to take the exam instead of the student, while at indirect substitution, the student takes the exam himself, but another person gives him the answers. Another important security issue during computer testing is cheating. A student can cheat by chatting with classmates in messengers or browsing the Internet. Different e-learning systems use different technologies to solve this problem. The main threats of academic virtue violation in e-learning systems and protection methods are given in tab. 13.

Table 13. Threats of academic integrity violation in e-learning systems

Threats	**Methods of protection**
Proxy test-taker	Biometric identification during authorization and during the test Online proctoring during the test
Cheating	Using Safe Exam Browser mode during the test Online proctoring during the test
Proxy attendance	Access only from a specific IP*/MAC address Access only from the internal network of the educational institution through a proxy server Blocking of simultaneous passing of several test
Passing the test after the allowed time	Restrictions on the start / end time of test availability Limitation on the duration of the test

* Not recommended for poor internet connection where frequent IP address updates are possible.

Safe Exam Browser (SEB) is a customizable web browser available for Windows, macOS, and iOS. It is licensed under the Mozilla Public License. The program runs on the student's computer and blocks all other applications except those necessary for taking the test. Network interaction takes place only through the SEB browser, which connects to the educational platform on which the test or exam is being conducted (e.g. Moodle). The program must be downloaded and installed on the device used by the student for testing. The restrictions imposed on students are similar to the “Full-screen pop-up with some JavaScript protection' restriction”. However, Safe Exam Browser, being software that runs on the student's device, offers additional features.

The principle of the Safe Exam Browser functioning is presented in fig. 9. Kiosk Application and Browser are the internal parts of the Safe Exam Browser.

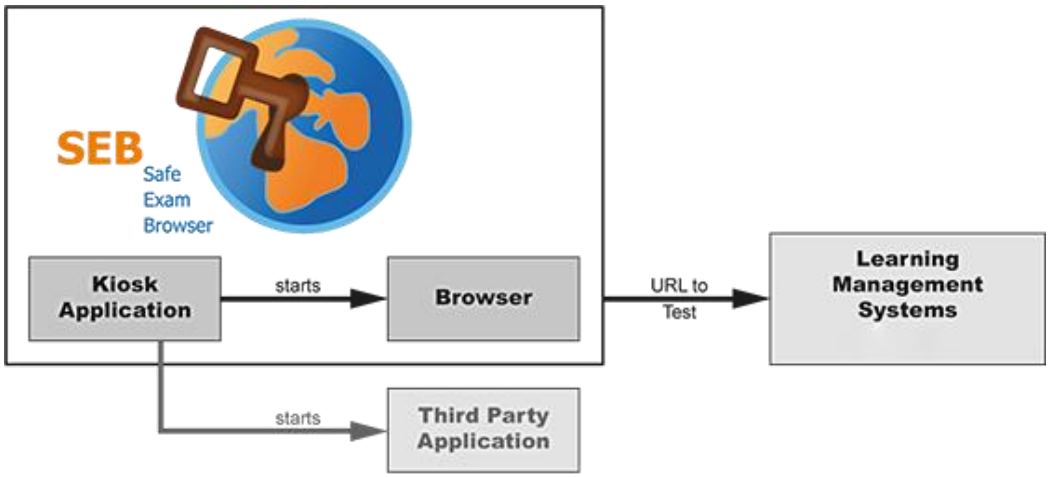


Fig. 9. Safe Exam Browser

Source: https://safeexambrowser.org

The main technical features of Safe Exam Browser mode are:

- There is possibility to take the exam only through the Secure Exam Browser;
- Switching to third-party applications is disabled by default, but it is possible allow the use of certain third-party applications during the exam, such as a calculator or Excel for calculations;
- There is no way to search for information in the browser concurrently because there is no address bar and search box, no navigation buttons, and no way to close the browser before the end of the test;
- Hotkeys are disabled or cannot be used for closing the browser or switching to other user accounts on the computer;
- The ability to take screenshots is disabled;
- The clipboard is cleared when the browser is opened and closed;

– Customization of access to specific sites, pages, and resources during the exam is possible using a URL filter;

– The application cannot be run on a virtual machine.

Safe Exam Browser restricts unauthorized device usage, but there is still a possibility of using third-party objects, devices, or receiving help from a friend.

Safe Exam Browser restricts unauthorized use of the device, but there is still a possibility of using third-party objects, devices, or help of a friend.

The settings used for the test are kept in the SEB configuration file. It is given to the student for access to the test attempt. It is possible to bypass these settings, e.g. by changing the browser's user-agent parameter or modifying the virtual machine configuration file to run SEB. Information on the SEB vulnerabilities is presented in papers of Søgaard Th.M. (*Søgaard Th.M., 2020*) and NeoBIT company blog (2016).

To prevent impersonation and cheating, a continuous monitoring system has been implemented to control students during exams.

Online proctoring, also known as e-monitoring, is a system used to verify compliance with exam regulations through automatic or semi-automatic monitoring. It detects prohibited actions during an online exam and ensures academic integrity through automatic surveillance from three sources: audio, video, and screen recording. This is similar to the observation of a teacher during an in-person exam. The system automatically records violations and sends the information to the e-learning system.

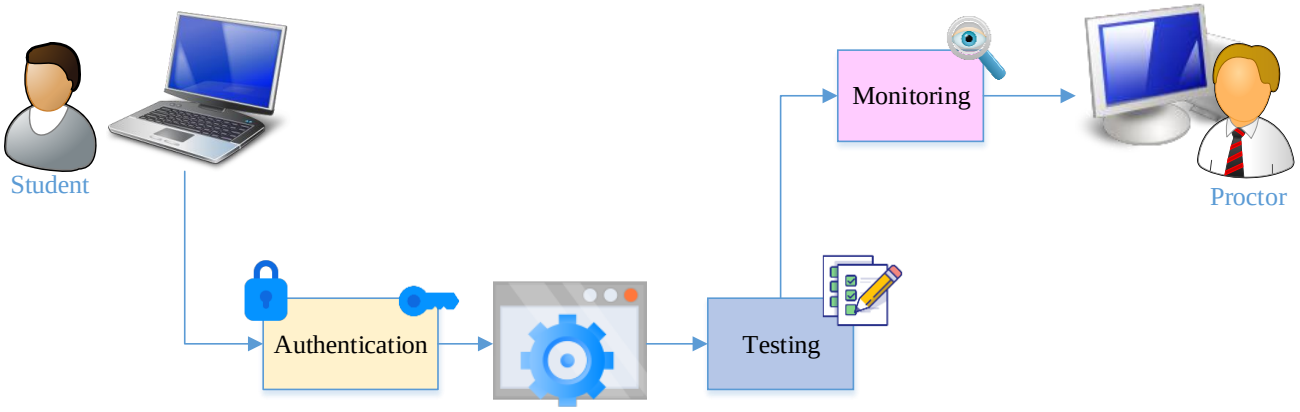


Fig. 10. Online proctoring

Online proctoring has various modes:

1. Automatic: The system automatically detects violations and issues a warning to the student. If the violations are serious or the student does not respond to the warning, the exam is stopped. The results are transferred to the testing system, which cancels the results with a low reliability rating.

The advantage of this method is low cost, but the disadvantage is the possibility of error.

2. Automatic asynchronous proctoring with post verification: The system automatically detects violations and issues a warning to the student. If serious violations occur or the student does not respond to the warning, the exam is marked as unreliable but not interrupted. The results are transferred to the testing system, and exams with low reliability ratings are manually checked. A final decision is made based on the results of the manual check. This method has several advantages, including low cost, the possibility of manual spot check. The disadvantage is the possibility of error.

1. Semi-automatic synchronous proctoring with a proctor: The system automatically detects violations and sends a message to the proctor, who is observing a group of students at the same time, indicating which student to focus on. The final decision to continue or stop the exam is made by the proctor. The advantages of this method are high accuracy and high cost.

The exam video is stored on the server. In case of an appeal or disagreement with the results, it is possible to view the exam video/screenshots in manual mode as the decision on violations during the exam is made by artificial intelligence, which can make mistakes. The main violations recorded by the system are: student absence or presence of another person in the frame; anomalies in the gaze direction or closing of the face part, conversation, use of third-party applications or tabs in the browser, connection of a second monitor, use of additional devices, books and notes, detection of broadcasting software, and detection of non-verbal communication.

Face recognition in proctoring systems is implemented using artificial intelligence, in particular convolutional neural networks.

Online proctoring offers several advantages, including automatic exam monitoring and possibility of simultaneous testing of a large group of students.

However, it also has some disadvantages. First, the integration of the online proctoring system with LMS is required at the API and UI level. This can be achieved in one of two ways: connecting the LMS to the proctoring system or adding proctoring functions to the LMS. Second, the availability of necessary additional equipment, such as main and additional webcams and a microphone, and the increased requirements for the computer technical parameters, particularly for internet bandwidth, may be unaffordable for students from low-income or rural areas.

Despite some disadvantages, online proctoring is one of the best solutions to protect against cheating during the exam.

Regulations on Security and Personal Data Protection in learning platforms

The Ukrainian legal framework. The legal basis for the processing and protection of personal data is established by the Law of Ukraine “On Personal Data Protection”, adopted on June 1, 2010. This law is crucial for learning systems in the context of processing and storing personal data

of students and teachers, as well as ensuring their confidentiality. The Law defines personal data as information or a set of information about an individual who is identified or can be identified. The provisions of this law refer primarily to classic personal data, such as full name, identification number, passport data, and basic biographical and contact information, which are socially acquired, i.e., assigned to a person in connection with public life, and can be changed. Biometric data can be considered as a distinct category of personal data, but this concept is not considered specifically in the law. Article 7 of this law prohibits the processing of biometric or genetic data if the personal data subject has not given unambiguous consent to the processing of such data.

The Law of Ukraine "On the Unified State Demographic Register and Documents Certifying Citizenship of Ukraine, a Person's Identity or Special Status" defines biometric data as a set of personal data collected based on recorded characteristics that are stable and significantly different from similar parameters of other persons. Biometric data includes digitized signatures, images of faces, and fingerprints. Biometric parameters are defined as measurable physical characteristics or personal behavioral traits that are used for identification (recognition) of a person or verification of provided identification information about a person.

As biometric data is considered a distinct category of personal data, its processing must comply with the Law of Ukraine "On Personal Data Protection" and the fundamental principles of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data No. 108, ratified by Ukraine on 06.07.2010 and entered into force for Ukraine on 01.01.2011.

Learning systems, especially in the online format, must comply with the information security requirements provided by the Law of Ukraine "On the Protection of Information Stored in Information and Telecommunication Systems" (date of adoption: 05.07.1994 (with changes). This law sets forth regulations for information protection in information and telecommunication systems (ITS), including access to information within the system (Article 4), conditions for information processing within the system (Article 8), and ensuring information protection within the system (Article 9), etc.

The Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" (current version on January 1, 2024) sets the basic principles and regulations in the area of cybersecurity. Educational systems must comply with its provisions in terms of developing and implementing of the cybersecurity policies, protecting information resources and systems from cyberattacks, and responding to cybersecurity incidents.

The European Union legal framework. In the European Union, the collection and transfer of personal data is governed by the EU data protection regulations, in particular GDPR from 2016 (entered into force May 25, 2018). General Data Protection Regulation (GDPR; Regulation (EU)

2016/679) is a general regulation on the protection of personal data of individuals within the European Union and the European Economic Area, which sets uniform rules for the protection of personal data of all EU citizens. Any learning systems that collect and process personal data of students must comply with the GDPR requirements for data agreement, storage, and processing.

According to Art. 4 of the GDPR personal data is any information relating to a "data subject", i.e. an identified or identifiable natural person; an identifiable natural person is an individual who can be directly or indirectly identified, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific for the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

In particular, this document highlights the concept of biometric data. According to GDPR biometric data are personal data obtained as a result of technical processing related to the physical, physiological or behavioral characteristics of a natural person, which allow to carry out or confirm the unique identification of the natural person, for example, facial image or dactyloscopic data.

According to Art. 25 of the GDPR, systems that process personal data must be built on the principle of "privacy by design and default," which means that personal data must be stored using pseudonyms or complete anonymization. The highest privacy level setting must be used by default so that the data is not publicly available without explicit consent and cannot be used for identification without additional information stored separately.

This regulation outlines the basic principles for handling personal data (Art. 5). In particular, the data minimization principle dictates that the system should store only data that is necessary for the fulfillment of a specific purpose, such as the educational process.

The information about the collection, using, viewing or processing of personal data concerning individuals should be transparent to those individuals. They should be informed how and to what extent their personal data will be processing. For example, the system should inform about video recording of the classes.

The limited storage principle means that personal data cannot be stored longer than necessary to fulfill the purpose for which it was collected, and that the information must be deleted after the purpose has been achieved. This means that students who have been expelled or graduated must be deleted from the system, otherwise their data may be compromised and they may get illegal access to the system. The right to delete data entitles the students to request the deletion of their information after graduation to prevent it from being shared with third parties. This principle overlaps with the principle of limited storage.

The EU Directive on Web Accessibility (Directive [EU] 2016/2102) concerns the accessibility of web and mobile application content for individuals with special educational needs, and the

compliance of the site with the WCAG 2.0 web content accessibility guidelines. In the context of electronic authentication, this means that the system must provide accessible authentication mechanisms for individuals with visual, hearing, cognitive, or motor impairments. This requirement is mandatory for public sector bodies in EU countries, including schools and universities.

The regulatory requirements for the protection of personal data in the European Union are more are more strict, as well as the responsibility for their violation.

Despite the active development of artificial intelligence and the biometric identification market, several legislative acts have been adopted since 2021 that limit the use of artificial intelligence technologies including systems for remote face recognition, except for military and judicial systems.

In the analysis "Regulating facial recognition in the EU", the European Parliament proposed to introduce new rules regulating the use of facial recognition technologies in the EU, and to divide them into "high-risk" and "low-risk" systems according to the characteristics of their use. Before being authorized for use, high-risk AI systems will be subject to particularly rigorous compliance checks.

The European Commission's press release “Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence”, published on April 21, 2021, consider artificial intelligence technologies used in education or professional training as high-risk systems, along with critical infrastructure objects, as these technologies can determine access to education and professional courses, such as exam assessment. Therefore, individuals must be aware that they are being recorded when using such systems, especially in online proctoring technology. They must give explicit consent for the personal data collection, and the system must ensure a high level of data protection and control.

The legal basis of biometric authentication is also discussed in the monograph “Legal framework of bioeconomy and biosecurity” (2021).

Conclusions. The issue of data security in e-learning systems is crucial. The main aspects of information security are confidentiality, integrity, and availability which violation leads to the system vulnerabilities and possibilities of cyberattacks. The key concepts of data control security and protection against unauthorized access are identification and authentication. The choice of a specific authentication method should be based on the desired accuracy and security characteristics, taking into account its cost, advantages and disadvantages, and comply with the legislation of the country in which the system is intended to be used. The integration of blockchain technology with learning systems is being considered as a means to secure student data and maintain the integrity of academic records within these systems.

It should be noted that authentication systems with a high level of protection involve the collection and storage of personal data, the compromise of which can have significant negative consequences for the data owner and lead to financial losses for the data operator for violating of security and confidentiality requirements.

In e-learning systems, it is recommended to use two-factor authentication to provide a sufficient level of protection and maintain the interface friendliness and the technical possibility of authentication for all social groups of students, including those with disabilities.

Most of the threats associated with the identification methods are attempts to get system access without user knowledge. At the same time, one of the key problems associated with e-learning systems is protection against identity-swap and cheating. Safe Exam Browser mode and online proctoring during the test, as well as restrictions associated with the testing place and time, are considered as effective tools against violating academic virtue in e-learning systems. The combination of these tools is an effective means but any control tool can be deceived and it is necessary to create such conditions so that it is easier and cheaper to pass an online exam honestly than fraud.

To ensure security from unauthorized access, in particular MITM attacks, it is recommended to use an encrypted connection and cryptographic methods during data transfer. An effective tool is combination of group cryptography with online proctoring.

Regular security audits and updates are also crucial in maintaining the integrity of learning systems.

Prospects for future research. Future research can be focused on the study of implementing multi-factor authentication to enhance security, effective algorithms of data encryption to protect sensitive information; use of artificial intelligence and machine learning algorithms to detect and respond to potential security threats in real-time within these systems.

References:

Al-azaiza R. (2016) Detection and Prevention of XSS Vulnerabilities in MOODLE. *Computer Science*, 2016.

Ally S. Review of Online Examination Security for the Moodle Learning Management System. *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*, vol. 18, issue 1, pp. 107-124, 2022.

Barhoom T.S.. Azaiza R.J (2016) Enhance MOODLE Security Against XSS Vulnerabilities. *International Journal of Computing and Digital Systems*, no. 5, pp. 421-430, 2016. http://dx.doi.org/10.12785/ijcds/050507.

Bhatia M., Maitra J.K (2018) E-learning Platforms Security Issues and Vulnerability Analysis. *2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES)*, Lucknow, India, pp. 276-285, 2018. DOI: 10.1109/CCTES.2018.8674115.

Briliyant O.C., Baihaqi A. (2017) Implementation of RSA 2048-bit and AES 128-bit for Secure e-learning web-based application. *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, Lombok, Indonesia, pp. 1-5, 2017. DOI: 10.1109/TSSA.2017.8272903.
Chatterjee P. et al. (2023). Enhancing Data Security of Cloud Based LMS. *Wireless Personal Communications*, vol. 130, pp. 1123–1139, 2023. https://doi.org/10.1007/s11277-023-10323-5.
Djeki E., Degila J. (2021) Bondiombouy C. and Alhassan M.H. Security Issues in Digital Learning Spaces. *2021 IEEE International Conference on Computing (ICOCO)*, Kuala Lumpur, Malaysia, pp. 71-77, 2021. DOI: 10.1109/ICOCO53166.2021.9673575.
MNet_Protocol. https://docs.moodle.org/dev/MNet_Protocol.
State of ransomware in education report. https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-education
Maynes M. One simple action you can take to prevent 99.9 percent of attacks on your accounts. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/
The Law of Ukraine. On the Basic Principles of Cybersecurity in Ukraine. https://zakon.rada.gov.ua/laws/show/en/2163-19#Text.
Phishing Activity Trends Report, 3rd Quarter 2022. https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf.
Гук О., Лоза В., Волошко С., Курчанов В. (2020) Підходи до організації захищеного доступу до систем дистанційного навчання вищих військових навчальних закладів із застосуванням VPN-мереж. *Збірник матеріалів ІІІ міжнародної науково-практичної конференції «Проблеми впровадження дистанційного навчання в освітньому процесі вищих військових навчальних закладів та можливі шляхи їх вирішення»*, с. 21- 25, 2020.
Фонар Л.С., Коновалов О.С., Філіппов Є.Г. (2022) Дослідження загроз інформаційної безпеки при використанні веб-технологій дистанційного навчання. *Прикладні питання математичного моделювання*. Том 5, № 1, с. 102-107, 2022. https://doi.org/10.32782/mathematical-modelling/2022-5-1-13.
IRONSCALES Releases Findings from State of Cybersecurity Survey. https://ironscales.com/blog/ironscales-releases-findings-from-state-of-cybersecurity-survey/
Закон України. Про захист інформації в інформаційно-комунікаційних системах. https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.
Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. https://zakon.rada.gov.ua/laws/show/994_326#Text.
1000 и 1 способ обойти Safe Exam Browser. Блог компании НеоБИТ. https://habr.com/ru/company/neobit/ blog/512678.
AbuMansour H.Y. (2017) Proposed Bio-authentication System for Question Bank in Learning Management Systemsю *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, pp. 489-494, 2017. DOI: 10.1109/AICCSA.2017.215.
Akacha S.A.-L. Awad A.I. (2023) Enhancing Security and Sustainability of e-Learning Software Systems: A Comprehensive Vulnerability Analysis and Recommendations for Stakeholders. *Sustainability*, 15(19), 14132, 27 pp., 2023. https://doi.org/10.3390/su151914132.
Alarape M., Saheed M. (2017) Enhancing computer based assessment security using biometric facial data. Circulation in Computer Science, vol. 2, no. 4, pp. 22-26. 2017. DOI: 10.22632/ccs-2017-252-04.
Al-Saleem S. M. Ullah H. (2014) A review of security considerations and palm based authentication scheme for computer based testing. *2014 9th International Conference on Computer Science & Education*, pp. 291-293, 2014. DOI: 10.1109/ICCSE.2014.6926472.
Apampa K., Wills G., Argles D. (2010) User security issues in summative e-assessment. *International Journal of Digital Society*, 1, pp. 1-13, 2010.

Article 4 GDPR. Definitions. https://gdpr-text.com/ru/read/article-4.
Asha S., Chellappan C. (2008) Authentication of e-learners using multimodal biometric technology. *2008 International Symposium on Biometrics and Security Technologies*, Isalambad, Pakistan, pp. 1-6, 2008. DOI: 10.1109/ISBAST.2008.4547640.
Beaudin Sh. (2016) An Empirical Study of Authentication Methods to Secure E-learning System Activities Against Impersonation Fraud. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (958), pp. 1-173, 2016.
Erlich Z., Zviran M. (2009) Authentication Methods for Computer Systems Security. *Encyclopedia of Information Science and Technology, Second Edition*. IGI Global, pp. 288-293, 2009. DOI: 10.4018/978-1-60566-026-4.ch049.
Europe fit for the Digital Age: Artificial Intelligence. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.
Evwiekpaefe A. E., Eyinla V. O. (2021) Implementing Fingerprint Authentication in Computer-Based Tests. *Nigerian Journal of Technology*, vol. 40, no. 2, pp. 284-291, 2021. http://dx.doi.org/10.4314/njt.v40i2.14.
Fouad K., Hassan B.M., Hassan M.F. (2016) User Authentication based on Dynamic Keystroke Recognition. *International Journal of Ambient Computing and Intelligence*, vol. 7, pp. 1-32, 2016. DOI: 10.4018/IJACI.2016070101.
Gao Q. (2012) Biometric authentication to prevent e-cheating. *International Journal of Instructional Technology and Distance Learning*, 9, pp. 3-13, 2012.
Haitan O. (2022) Comparative analysis of possibilities of using the toolkit of webinar-based platforms Zoom, Google Meet and Microsoft Teams in online-learning. *Information Technologies and Learning Tools*, vol. 87(1), pp. 33–67, 2022. DOI: 10.33407/itlt.v87i1.4441.
Hoffman A. (2020). Web Application Security. Exploitation and Countermeasures for Modern Web Applications. Sebastopol, O'Reilly Media, pp. 27-28, 2020.
Huszti A., Petho A. (2010) A secure electronic exam system. *Publications Mathematician Debrecen*, vol. 77, no 3-4, pp. 299-312, 2010. DOI: 10.5486/PMD.2010.4682
Ibrahim M. et al. (2017) Design of a fingerprint biometric authentication technique for electronic examination. *International Journal of Computer Science and Telecommunications*, vol. 8, no. 2, pp. 8–15, 2017.
Sun H., Wang X., Wang, X. (2018). Application of Blockchain Technology in Online Education. *International Journal of Emerging Technologies in Learning*, vol. 13, no. 10, pp. 252-259, 2018. https://doi.org/10.3991/ijet.v13i10.9455.
Jagadamaba G., SathishBabu B. (2019) Keystroke Dynamics in E-Learning and Online Exams. *Biometric Authentication in Online Learning Environments*, pp. 1-21, 2019. DOI: 10.4018/978-1-5225-7724-9.ch001.
Curran J., Curran K. (2021) Biometric Authentication Techniques in Online Learning Environments. In book *Research Anthology on Developing Effective Online Learning Courses*, chapter 42, IGI Global, 13 pp., 2021. DOI: 10.4018/978-1-7998-8047-9.ch042.
Ko C.C., Cheng C.D. (2008) Flexible and secure computer-based assessment using a single zip disk. Computers & Education, 50(3), pp. 915-926, 2008. https://doi.org/10.1016/j.compedu.2006.09.010.
Laamanen M. et al. (2021) Acceptability of the e-authentication in higher education studies: views of students with special educational needs and disabilities. International Journal of Educational Technology in Higher Education, vol. 18, 4, 2021. https://doi.org/10.1186/s41239-020-00236-9 .
Lee Aeri, Han Jin-young (2020) Effective User Authentication System in an E-Learning Platform. *International Journal of Innovation, Creativity and Change*, vol. 13, issue 3, pp. 1101-1113, 2020.
Luu Q. et al. (2020) Authentication in E-learning systems: Challenges and Solutions. *VNUHCM Journal of Engineering and Technology*, 3(SI1), pp. SI95-SI101, 2020. DOI: 10.32508/stdjet.v3iSI1.516

Machani S. et al, FIDO UAF Architectural Overview. FIDO Alliance, 2017.
Meyer D. Europe's privacy regulators call for a ban on facial recognition in publicly accessible spaces. https://fortune.com/2021/06/21/ban-facial-recognition-in-all-publicly-accessible-spaces-europe-privacy-regulators-urge-edps-edpb-ai-regulation/.
Moini A., Madni A.M. (2009) Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective. *IEEE Systems Journal, Special issue on Biometrics Systems*, vol. 3, no. 4, pp. 469-476, 2009. DOI: 10.1109/JSYST.2009.2038957.
Odeh N., Hijazi Sh. (2023) Detecting and Preventing Common Web Application Vulnerabilities: A Comprehensive Approach. International Journal of Information Technology and Computer Science, no. 3, pp. 26-41, 2023. DOI: 10.5815/ijitcs.2023.03.03.
Okada A. et al. (2019) E-Authentication for online assessment: A mixed-method study". *British Journal of Educational Technology*, vol. 50, no. 2, pp. 861-875, 2019. DOI:10.1111/bjet.12608.
Ramu T., Arivoli T. (2013) A framework of secure biometric based online exam authentication: an alternative to traditional exam. *Int J Sci Eng Res*, 4 (11), pp. 52-60, 2013.
Rao N.S.S. et al. (2011) Cryptography – Analysis of Enhanced Approach for Secure Online Exam Process Plan. *International Journal of Computer Science and Telecommunications*, vol. 2, issue 8, pp. 52-57, 2011.
Regulating facial recognition in the EU. https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf.
Rudrapal D. et al. (2012) Voice Recognition and Authentication as a Proficient Biometric Tool and Its Application in Online Exam for P.H People. *International Journal of Computer Applications*, vol. 39, 02, pp. 6-12, 2012. DOI: 10.5120/4870-7297.
Søgaard Th.M. Mitigation of Cheating Threats in Digital BYOD exams. Norwegian University of Science and Technology, 120 pp., 2020.
Safe Exam Browser. https://docs.moodle.org/311/en/Safe_Exam_Browser.
Salameh N., Shukur Z. (2015) Review of user authentication methods in online examination. *Asian Journal of Information Technology*, 14, pp. 166-175, 2015. DOI: 10.3923/ajit.2015.166-175
Shdaifat A., etc. (2020) A proposed Iris Recognition Model for Authentication in Mobile Exams. International Journal of Emerging Technologies in Learning (iJET), vol. 15(12), pp. 205-216, 2020. DOI:10.3991/ijet.v15i12.13741
The State of Ransomware in Education 2023. https://news.sophos.com/en-us/2023/07/20/the-state-of-ransomware-in-education-2023/
Timirgaleeva R.R., Grishin I.Yu., Mironov M.V. (2019) E-Learning: the Problem of Reliable Student Authentication and Information Security. Selected *IV All-Russian scientific and practical conference with international participation "Information Systems and Technologies in Modeling and Control" (ISTMC'2019)*, pp. 213-223, 2019.
Ullah A. et al. (2012) Using Challenge Questions for Student Authentication in Online Examination. *International Journal for Infonomics*, vol. 5, pp. 631-639, 2012. DOI: 10.20533/iji.1742.4712.2012.0072.
Ullah A. et al. (2014) Evaluating security and usability of profile based challenge questions authentication in online examinations. *Journal of Internet Services and Applications* 5, 2, 2014. https://doi.org/10.1186/1869-0238-5-2.
Yaseen K.A.Y. (2023) Enhance MOODLE Platform Security Against Denial of Service Attack (DoS). *Journal of Critical Reviews*, vol. 10, issue 02, pp. 140-147, 2023. DOI: 10.31838/jcr.10.02.16.
Zamfiroiu A. et al. (2020) Secure Learning Management System Based on User Behavior. *Applied Sciences*, vol. 10(21), pp. 7730, 2020. DOI: 10.3390/app10217730.
Биометрия от «А» до «Я» полное руководство биометрической идентификации и

аутентификации. https://securityrussia.com/blog/biometriya.html.
Европарламент призвал запретить системы распознавания лица. https://www. securitylab.ru/news/525333.php
Ігнатович А.О. (2016) Методи підвищення ефективності компонентів безпеки комп'ютерних систем з використанням маскуючих елементів текстових та біометричних даних, Львів, 145 с, 2016.
Онлайн-прокторинг: для кого, зачем и как он работает. https://ru.examus.net/online-proctoring.
Правовые основы биоэкономики и биобезопасности, М.: Проспект. С. 1-480, 2021.
Пересыпкин и др. (2016) Принципы работы и уязвимости биометрических систем аутентификации. *Молодой ученый*, № 30 (134), с. 86-88, 2016.
Прокторинг на стероидах, или как контролировать онлайн-экзамены. https://www.croc.ru/news_posts/kak_kontrolirovat_onlajn-ekzameny/

DOI 10.5281/zenodo.10822085
UDC 004.738

CHAPTER 21.
VIRTUAL PRIVATE NETWORK BASED ON A SINGLE PLATE COMPUTER

Vladyslav NEBESNIUK
Software Engineer,
Zaporizhzhia, Ukraine
oyn1973@gmail.com
https://orcid.org/0009-0000-9217-3619

Abstract. VPN, or Virtual Private Network, is a general name for technologies that allow you to create a secure, encrypted Internet connection when a user is online. Today, the relevance of these technologies is beyond doubt. The war in Ukraine limited the right to access information for a certain category of Ukrainians. With the help of VPN technologies, you can easily bypass the blocking of content, entire sites, and services. VPN is also relevant when connecting to public networks and access points (the same Wi-Fi in a cafe or airport). VPN services encrypt your online data and protect your personal information. Many people work remotely these days, and many companies connect remote employees via VPN, as if they were all using the same local network in the office. Thanks to this, problems with access and protection of confidential data of companies are solved. Therefore, the use of a virtual private network will ensure the protection and privacy of a person while using the Internet. Therefore, the development of a virtual private network system on the basis of a single-board computer is quite an urgent issue.

Keywords: information, vpn, proxy server, privacy, security, network, raspberry pi, python, single plate computer

ВІРТУАЛЬНА ПРИВАТНА МЕРЕЖА
НА БАЗІ ОДНОПЛАТНОГО КОМП'ЮТЕРА

Анотація. VPN або віртуальна приватна мережа ─ це узагальнена назва для технологій, які дають змогу створити безпечне зашифроване інтернет-з'єднання під час виходу користувача в мережу *(Що таке VPN і яка його актуальність у наш час. ROOT NATIONAL, 2024. URL: https://is.gd/R4rG5W (дата звернення: 03.02.2024)).* Сьогодні актуальність цих технологій не викликає сумніву. Війна в Україні обмежила право на доступ до інформації певній категорії українців. За допомогою VPN технологій можна легко обходити блокування

контенту, цілих сайтів, сервісів. Також VPN актуальний під час під'єднання до загальнодоступних мереж і точок доступу (той самий Wi-Fi у кафе або аеропорту). VPN-сервіси шифрують ваші онлайн-дані та захищають вашу особисту інформацію. Зараз багато людей працюють віддалено, багато компаній під'єднують віддалених співробітників через VPN, так, як якщо б вони всі використовували одну й ту саму локальну мережу в офісі. Завдяки цьому вирішуються проблеми з доступом і захистом конфіденційних даних компаній. Тож застосування віртуальної приватної мережі дозволить забезпечити захист та конфіденційність особи під час користування Інтернетом**.** Тож розробка системи віртуальної приватної мережі на базі одноплатного комп'ютера є достатньо актуальним питанням.

Вступ. Не зважаючи на переваги, віртуальні приватні мережі мають і певні недоліки.

Використання VPN може дещо знизити швидкість з'єднання. Деякі VPN-сервіси значно знижують швидкість Інтернету, інші — лише незначним чином, а топові сервіси роблять цю затримку майже непомітною. Сповільнення з'єднання обумовлюється шифруванням даних та їх відправленням на сервер VPN, що вимагає часу.

Деякі VPN-сервіси можуть поставити під загрозу конфіденційність користувача. Краще обирати сервіс, який дотримується суворої політики відсутності журналів входу, перевіреної незалежними компаніями із забезпечення кібербезпеки.

Користування VPN не є безкоштовним. VPN є сервісами на основі підписки, які регулярно стягують плату за свої послуги. Проте користування більшістю цих сервісів коштує лише кілька доларів на місяць, тож насправді вони досить доступні. Крім того, вони, як правило, пропонують гарантію повернення коштів, що дозволяє спочатку випробувати їхні послуги, а потім, протягом встановленого терміну, отримати відшкодування коштів. Таким чином, користувачу не доведеться оформлювати підписку, доки він не пересвідчитеся, що сервіс йому підходить.

Погані VPN-сервіси мають обмежену мережу серверів та кількість IP-адрес. Деякі з них використовують маленькі серверні мережі або застарілу інфраструктуру. Якщо VPN не здатен оновлювати свої IP-адреси та сервери, це, ймовірно, буде негативно впливати на швидкість та значно обмежувати доступ користувача до потокового контенту.

Деякі країни обмежують або забороняють використання VPN-сервісів. Такі країни як Китай, Росія та Іран частково обмежують або навіть забороняють користування VPN *(Посібник з VPN: що таке VPN-з'єднання та як воно працює? VPN WIKI. URL: https://is.gd/mygQrg (дата звернення: 03.02.2024))*.

Ще однією технологією, що виконує функцію посередника між Інтернетом і користувачем є використання проксі-сервера. Проксі-сервер — це інший сервер, який

представляє пристрій користувача в Інтернеті. Він виконує роль посередника між пристроєм і веб-сайтами чи онлайн-службами. У разі підключення до нього всі вихідні та вхідні дані користувача проходять через проксі-сервер**.** Ваша IP-адреса замінюється IP-адресою сервера, при цьому всі онлайн-системи «думають», що ви підключаєтеся з сервера, а не зі свого пристрою (*Проксі-сервер: що це таке і чи потрібен він вам? Surfshark. URL: https://surfshark.com/uk/blog/proxy-server (дата звернення: 03.02*.2024)).

Автором проведено порівняння технологій VPN та проксі-сервера (табл.1) яке показало, що вони схожі тільки за принципом своєї роботи на базовому рівні - тим, що перенаправляють трафік даних через зовнішній сервер і змінюють IP-адресу користувача. Відрізняються ці технології двома ключовими компонентами - протоколами, які використовують для забезпечення конфіденційності дій користувача у мережі, та алгоритмами шифрування даних.

Таблиця 1- Порівняння технологій проксі і VPN

Проксі-сервер	VPN
Скеровує трафік користувача у браузері	Скеровує весь трафік пристрою користувача
Може приховувати IP-адресу користувача	Приховує IP-адресу користувача
Може мати шифрування	Шифрує усі дані користувача

Огляд літератури та методик. Віртуальна приватна мережа дозволяє забезпечити одне або кілька мережних з'єднань (логічну мережу) поверх іншої мережі (наприклад, Інтернет) (рис 1).

При підключенні до Інтернет через VPN-додаток на пристрої користувача (його ще називають VPN-клієнтом) між його пристроєм і VPN-сервером встановлюється безпечне з’єднання. Трафік проходить через провайдера клієнта, але він не може його прочитати або побачити кінцевий пункт призначення. Веб-сайти, які відвідує користувач, більше не бачать його вихідну IP-адресу, а бачать тільки IP-адресу VPN-сервера, яка спільно використовується багатьма іншими користувачами і регулярно змінюється.

Рис. 1 – Схематичне зображення віртуальної приватної мережі

(Yee C. K., Zolkipli M. F. Review on Confidentiality, Integrity and Availability in Information Security. // Journal of ICT in Education.- 2021.- Vol. 8.- P.34-42).

Залежно від застосовуваних протоколів і призначення, VPN може забезпечувати з'єднання трьох видів: вузол-вузол, вузол-мережу та мережу-мережу *(Технології забезпечення безпеки мережевої інфраструктури: підручник / В. Л. Бурячок та інш. Київ.: КУБГ, 2019. -218 с).*

Сучасні види VPN підключення :

OpenVPN — протокол з відкритим вихідним кодом, який відрізняється своєю надійністю та безпечністю. Відкритий вихідний код означає, що його програмний код є загальнодоступним, і тому будь-хто може перевірити його на міцність та надати власні рекомендації, які допоможуть зробити протокол ще безпечнішим. Він дуже популярний серед користувачів і шифрує трафік з обох боків, тобто лише відправник і одержувач мають ключ шифрування. Також він регулярно оновлюється та вдосконалюється, що додатково підвищує рівень його безпеки.

WireGuard — ще один протокол з відкритим кодом, швидший, ніж OpenVPN, і в той самий час не менш безпечний. Рекомендується використовувати його для потокової передачі, онлайн-ігор та відео дзвінків. Проте він може мати невиявлені вразливості, оскільки є відносно новим.

IKEv2 — надійний протокол зі швидкістю на рівні OpenVPN. Цей протокол дуже стабільний в роботі, тому він зможе захистити користувача навіть під час переходу з мобільної мережі на Wi-Fi. Однак він менш безпечний, ніж OpenVPN та WireGuard, тому його краще використовувати як резервний варіант.

SSTP — досить старий протокол для Windows, схожий за принципом роботи на OpenVPN, оскільки лише одержувач і відправник мають ключі для розшифрування з’єднання.

Це дозволяє ефективно долати системи контролю трафіку, проте швидкість його роботи дещо занизька.

L2TP/IPSec — застарілий протокол, який в основному використовується на смартфонах. Він не шифрує дані та працює дуже повільно, тому його краще уникати.

VPN класифікують за кількома основними параметрами *(Що таке VPN-підключення і як працює VPN? Самоосвіта URL: https://samoosvita.in.ua/scho-take-vpn-pidklyuchennya-i-yak-pratsyue-vpn (дата звернення: 05.02. 2024)*:

1. За ступенем захищеності використовуваного середовища

1.1. Захищені

Найбільш поширений варіант віртуальних приватних мереж. З його допомогою можливо створити надійну і захищену мережу на основі ненадійної мережі, як правило, Інтернету. Прикладом захищених VPN є: IPSec, OpenVPN і PPTP.

1.2. Довірчі

Використовуються у випадках, коли передавальну середу можна вважати надійною і необхідно вирішити лише завдання створення віртуальної підмережі в рамках більшої мережі. Проблеми безпеки стають неактуальними. Прикладами подібних рішень VPN є: Multi-protocol label switching (MPLS) і L2TP (Layer 2 Tunnelling Protocol) (точніше буде сказати, що ці протоколи перекладають завдання забезпечення безпеки на інші, наприклад L2TP, як правило, використовується в парі з IPSec).

2. За способом реалізації

2.1. У вигляді спеціального програмно-апаратного забезпечення

Реалізація мережі VPN здійснюється за допомогою спеціального комплексу програмно-апаратних засобів. Така реалізація забезпечує високу продуктивність і, як правило, високий ступінь захищеності.

2.2. У вигляді програмного рішення

Використовують персональний комп'ютер зі спеціальним програмним забезпеченням, що забезпечує функціональність VPN.

2.3. Інтегроване рішення

Функціональність VPN забезпечує комплекс, що вирішує також завдання фільтрації мережевого трафіку, організації мережевого екрану і забезпечення якості обслуговування.

3. За призначенням

3.1. Intranet VPN

Використовують для об'єднання в єдину захищену мережу декількох розподілених філій однієї організації, які обмінюються даними по відкритих каналах зв'язку.

3.2. Remote Access VPN

Використовують для створення захищеного каналу між сегментом корпоративної мережі (центральним офісом або філією) і одиночним користувачем, який, працюючи вдома, підключається до корпоративних ресурсів з домашнього комп'ютера, корпоративного ноутбука, смартфона або інтернет-кіоску.

3.3. Extranet VPN

Використовують для мереж, до яких підключаються «зовнішні» користувачі (наприклад, замовники або клієнти). Рівень довіри до них набагато нижче, ніж до співробітників компанії, тому потрібне забезпечення спеціальних «кордонів» захисту, що запобігають або обмежують доступ останніх до особливо цінної, конфіденційної інформації.

3.4. Internet VPN

Використовується для надання доступу до інтернету провайдерами, зазвичай якщо по одному фізичному каналу підключаються кілька користувачів. Протокол PPPoE став стандартом в ADSL-підключенні.

3.5. L2TP

Був широко поширений в середині 2000-х років в будинкових мережах: в ті часи внутрішньо трафік не оплачувалася, а зовнішній коштував дорого. Це давало можливість контролювати витрати: коли VPN-з'єднання вимкнено, користувач нічого не платить. В даний час провідний інтернет дешевий або безлімітний, а на стороні користувача часто є маршрутизатор, на якому вмикати-вимикати інтернет не так зручно, як на комп'ютері. Тому L2TP-доступ відходить в минуле.

3.6. Client / Server VPN

Він забезпечує захист переданих даних між двома вузлами (не мережами) корпоративної мережі. Особливість даного варіанту в тому, що VPN будується між вузлами, що перебувають, як правило, в одному сегменті мережі, наприклад, між робочою станцією і сервером. Така необхідність дуже часто виникає в тих випадках, коли в одній фізичній мережі необхідно створити кілька логічних мереж. Наприклад, коли треба розділити трафік між фінансовим департаментом та відділом кадрів, які звертаються до серверів, що знаходяться в одному фізичному сегменті. Цей варіант схожий на технологію VLAN, але замість поділу трафіку використовується його шифрування.

4. За типом протоколу

Існують реалізації віртуальних приватних мереж під TCP / IP, IPX і AppleTalk. Але на сьогоднішній день спостерігається тенденція до загального переходу на протокол TCP / IP, і

абсолютна більшість рішень VPN підтримує саме його. Адресація в ньому найчастіше вибирається відповідно до стандарту RFC5735, з діапазону Приватних мереж TCP / IP.

5. За рівнем мережевого протоколу

За рівнем мережевого протоколу на основі зіставлення з рівнями еталонної мережевої моделі ISO / OSI.

Розглянемо алгоритм роботи проксі-сервера *(Що таке проксі-сервер. Hosting Ukraint. URL: https://is.gd/olaSI9 (дата звернення: 05.02. 2024))*:

- користувач вводить адресу веб-сайту у своєму браузері;
- проксі-сервер отримує цей запит;
- проксі-сервер спрямовує запит на веб сервер, до якого користувач намагається підключитися;
- веб сервер надсилає відповідь (дані веб-сайту) назад на проксі-сервер;
- проксі-сервер пересилає відповідь користувачу.

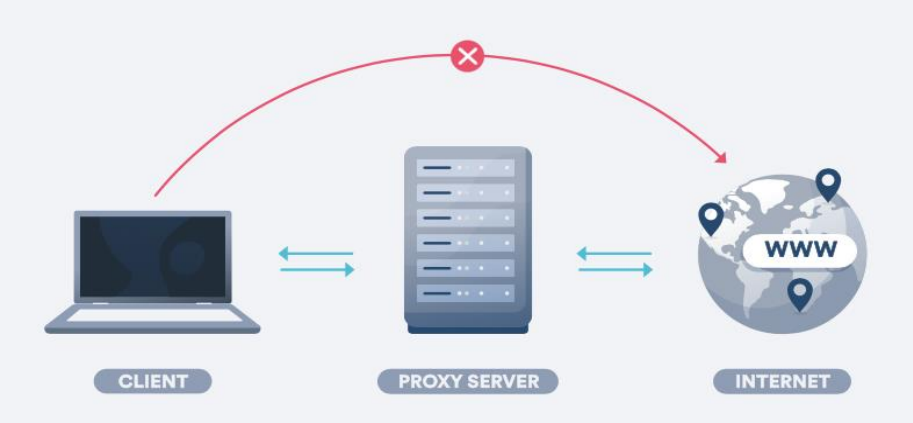


Рис. 2 – Принцип застосування проксі-сервера

Типи проксі-серверів *(Dsfferent Types if Proxy Servers and Their Uses. Securiwiser. URL: https://is.gd/J5ewRJ (дата звернення: 05.02. 2024))*:

Прямий (звичайний) проксі-сервер (рис. 3): найпоширеніший тип проксі — це посередник, що пересилає дані користувача від його імені. Окрім того, цей проксі забезпечує певний рівень захисту, оскільки не перенаправляє трафік доти, доки дані не будуть перевірені та визначені безпечними.

Зворотний проксі-сервер (рис.4): використовується веб сервером (тому і називається зворотним). Веб сервери (постачальники послуг) використовують зворотні проксі для кешування та отримання необхідних даних. Завдяки цим діям вони забезпечують безперебійність роботи для користувачів та зменшують навантаження на свої служби. Користувач не знає, що підключаєтеся до нього, але він може збирати необхідні дані з декількох

сайтів і потім передавати їх користувачу (за принципом «об'єднаної доставки» з онлайн-магазинів).

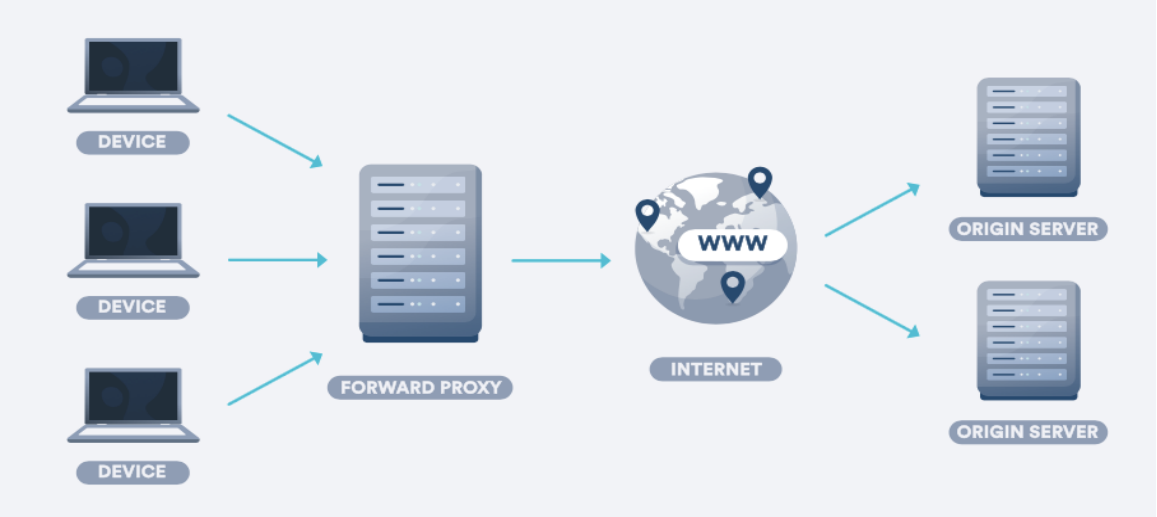


Рис.3 – Реалізація прямого проксі-сервера

Проксі з посиленою анонімністю**:** приховує як вихідну IP-адресу, так і факт використання проксі-сервера, регулярно змінюючи IP-адреси і не маючи в заголовку даних, що його розкривають.

Прозорий проксі-сервер**:** називається так через свою непомітність для користувача. Фактично він не змінює онлайн-запити та використовується для відстеження використання Інтернету й обмеження доступу. Їх часто використовують роботодавці, щоб контролювати своїх співробітників та не давати їм «гуляти по мережі» замість виконання робочих завдань. Можуть використовуватися також публічними бібліотеками.

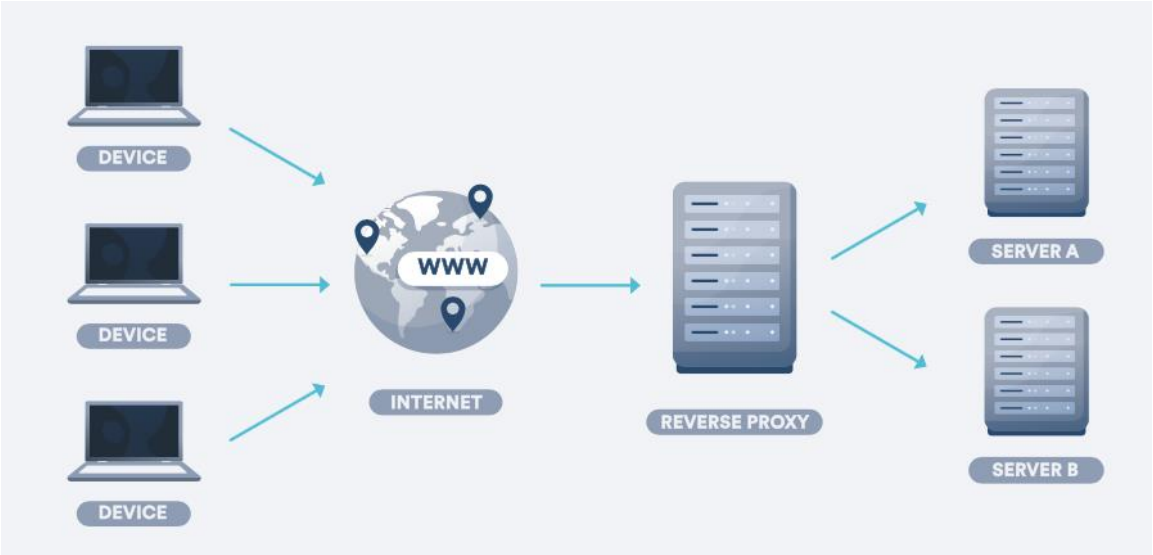


Рис. 4 – Реалізація зворотного проксі-сервера

CGI-проксі (загальний шлюзовий інтерфейс)**:** ця технологія підключається до проксі-сервера через веб-сайт. Користувач заходить на проксі-сайт CGI, вводить адресу потрібного

сайту у веб форму, і він відображається на сторінці проксі-сайту — виходить схоже на браузер у браузері. Якщо у користувача немає доступу до налаштувань проксі або пристрій не підтримує таку функцію, то CGI-проксі — підходяще рішення.

Суфікс-проксі**:** додає закінчення (суфікс) до адреси сайту задля обходу фільтрів брандмауера (проте сучасні фільтри можуть блокувати такі запити).

DNS-проксі (Domain Name System — «система доменних імен»)**:** комп'ютери використовують DNS для перекладу домашньої адреси веб сторінки з людської мови на цифрову — наприклад, з surfshark.com на 104.18.120.34 (IP-адреса). Проксі-сервер DNS обробляє, дозволяє або блокує всі DNS-запити. Наприклад, в разі введення Surfshark.com DNS вибере, який із серверів Surfshark буде виконувати цей запит.

Таким чином, на думку автора, найкращим підходом є використання змішаної моделі, яка комбінує переваги обох технологій. Це дозволить користувачам забезпечити високий рівень приватності, шифрування та анонімності завдяки VPN, а також використовувати проксі-сервери для додаткової прихованості їхньої реальної IP-адреси. Такий підхід буде особливо ефективним для тих випадків, коли важливо забезпечити якісний захист особистої інформації та одночасно мати можливість обходити географічні обмеження.

Мета розробки та дослідження. Автором пропонується віртуальна приватна система повного циклу яка дозволить користувачам забезпечити високий рівень приватності, шифрування та анонімності завдяки VPN, а також використовувати проксі-сервери для додаткової прихованості їхньої реальної IP-адреси.

Структурна схема (рис.5) наочно демонструє логічний зв'язок між елементами системи та дозволяє пояснити принцип їх роботи та функціональне призначення.

Користувач за допомогою персонального комп'ютера по мережі зв'язується з "Панеллю управління". Це звичайний веб-сайт, за допомогою якого можна гнучко керувати усіма частинами розробленої системи. За допомогою API інтерфейсу "Панель управління" пов'язана з "Головним сервером". "Головний сервер" контролює усі мережеві процеси та за допомогою асинхронної комунікації вміє спілкуватись з системами Raspberry Pi через маршрутизатор. В свою чергу Raspberry Pi 3 має інтерфейси (USB) для спілкування з модемами та має змогу виконувати певні команди, які відносяться до фінальних пристроїв.

Результати та обговорення. Для системи віртуальної приватної мережі (VPN) на базі одноплатного комп'ютера RASPBERRY PI 3 в якості панелі управління пропонується застосувати систему Typical Proxy. ЇЇ можна використовувати як проксі, VPN та отримувати смс-повідомлення в месенджері Telegram *(Typical Proxy. Brightdata. URL: https://is.gd/8IbjQR (дата звернення: 06.02. 2024)).*

Для входу необхідно мати логін і пароль (рис.6). Потім можливо перейти на сторінку панелі і ввести їх, щоб отримати доступ до панелі керування. Під час входу користувач бачить головну сторінку, що має автоматичне оновлення або інформаційну панель з основною інформацією.

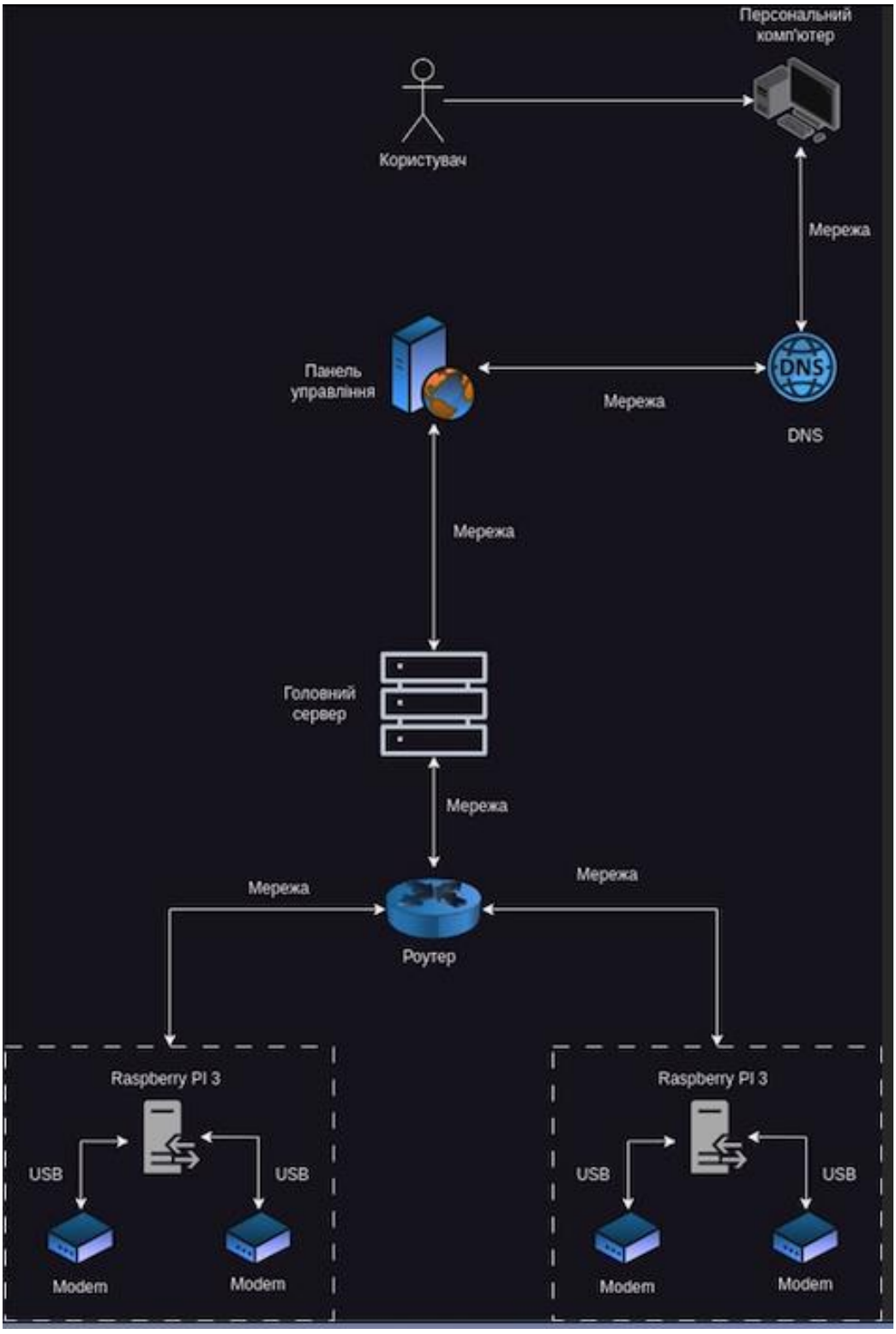


Рис. 5 – Структурна схема віртуальної приватної мережі (VPN) на базі одноплатного комп'ютера RASPBERRY PI 3

У лівій колонці відображаються активні підключення в представленій системі (рис.7):

0 хвилин - час сесії

213.108.199.134 - IP-адреса користувача, який створив цей сеанс

46.133.193.125 - публічна IP-адреса, яку користувач отримує, коли будете використовувати цей сеанс. Червона іконка - додавання загальнодоступного IP до чорного списку

46.175.249.195:50005 - адреса проксі лише для інформації

Активне з'єднання може бути створено, тільки якщо IP-адреса користувача є у списку дозволу.

В центральній колонці головної сторінки представлена панель керування IP, де можливо додати нові IP-адреси до списку дозволу (тоді користувач матимете доступ для використання проксі-сервера) або чорного списку (лише загальнодоступні IP-адреси, які використовуються для реєстрації).

У правій колонці головного вікна представлені деталі проксі-сервера для підключення. Тут можливо використовувати IP та порт проксі-сервера для підключення до запропонованої системи. Також перевірити, чи активна система чи ні та як довго.

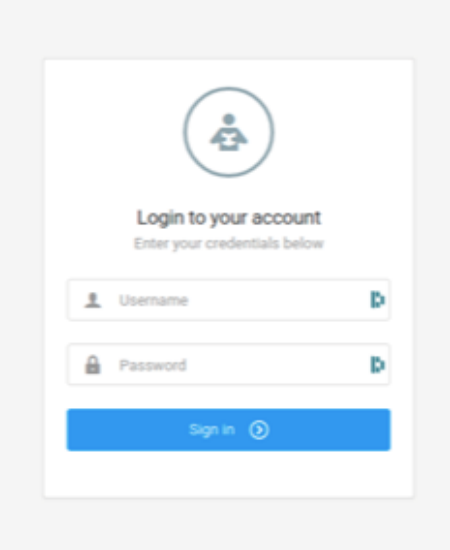


Рис.6 -Вигляд вікна для аутентифікації

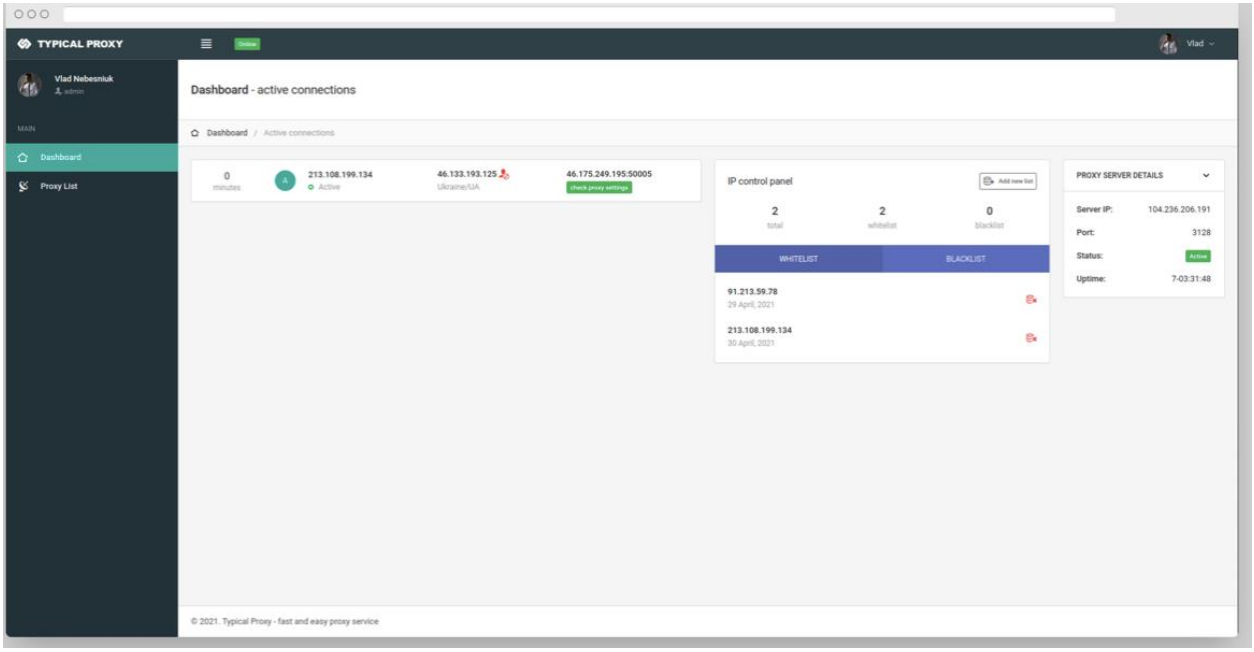


Рис. 7- Головне вікно програмного застосунку

На другій сторінці головного вікна (рис.8) користувач може перевірити всі доступні модеми для використання та, за необхідності, ввести відповідні зміни (оновити номер телефону, отримати нові sms, редагувати або видалити проксі).

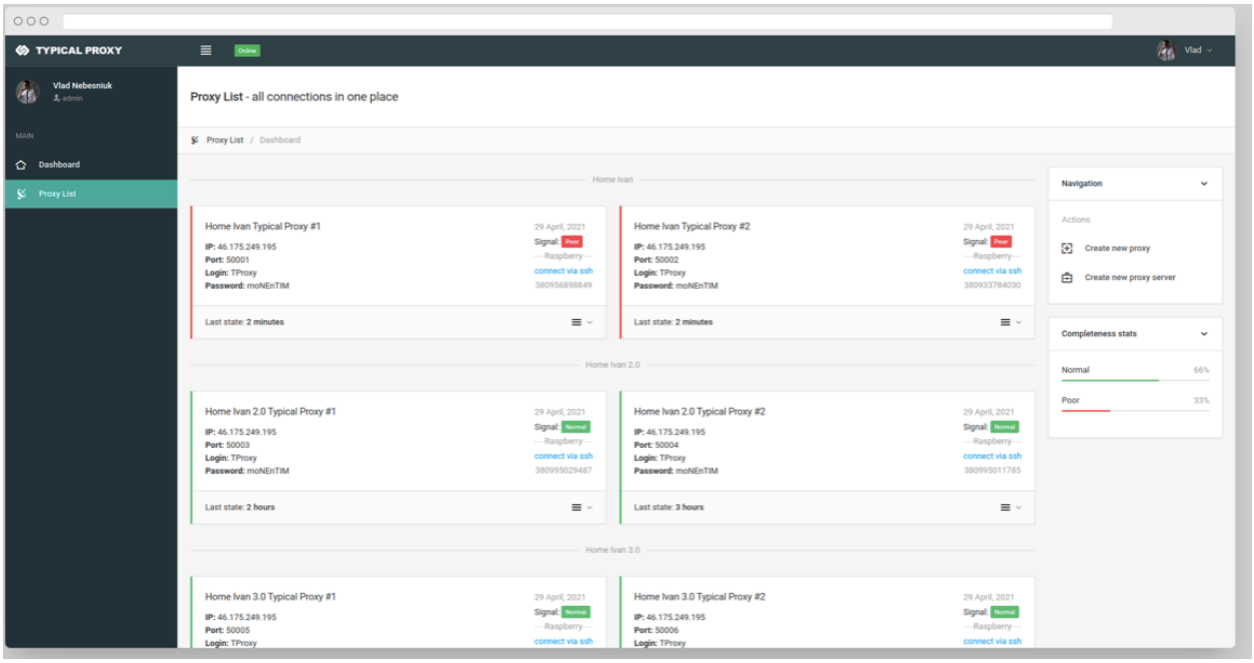


Рис. 8- Модеми, доступні до використання

В якості проксі-серверу використовується міні-комп'ютер Raspberry PI 3, який керує двома модемами. В якості проксі – модему обрано Huawei e3372h.

Щоб використовувати проксі необхідно додати свій IP до списку дозволу. Для цього:

Firefox

- запустіть Firefox
- перейдіть до Налаштування --> Налаштування мережі
- натисніть Налаштування проксі вручну
- введіть HTTP-проксі з IP 104.236.206.191 і портом 3128
- встановити прапорець Використовувати цей проксі для FTP і HTTPS
- натисніть OK
- закрийте Firefox

Chrome

- запустіть Google Chrome
- перейдіть до Параметри --> Додатково --> Система --> Відкрити налаштування проксі
- вимкнути автоматичне визначення параметрів
- включити Використовувати проксі-сервер
- введіть IP 104.236.206.191 і порт 3128
- натисніть Зберегти
- закрийте Google Chrome
- вимкніть Використовувати проксі-сервер

Для налаштування проксі-серверу необхідно виконати кілька кроків:

- придбати Rasbperry, модеми, ethernet кабель, кабель живлення
- підключення модемів і Rasbperry через USB-порт
- підключіть домашній маршрутизатор за допомогою кабелю Ethernet
- підключіть Rasbperry до кабелю живлення

Тепер необхідно зробити деякі порти публічними, щоб отримати доступ ззовні:

- підключитися до домашньої мережі WIFI
- перейти на сторінку http://192.168.0.1 і ввести логін admin і пароль admin
- перейти до DHCP -> Список клієнтів DHCP і знайти малину та її IP-адресу

Потім перейти до розділу NAT Redirect -> Virtual Servers і створити кілька нових рядків:

- сервісний порт 22, IP-адреса -> rasbperry IP-адреса, внутрішній порт 22, протокол TCP
- сервісний порт 8333, ip-адреса -> IP-адреса rasbperry, внутрішній порт 8333, протокол TCP
- порт служби 50001, ip-адреса -> IP-адреса rasbperry, внутрішній порт 50001, протокол TCP

- порт служби 50002, ip-адреса -> IP-адреса rasbperry, внутрішній порт 50002, протокол TCP

Наступним кроком необхідно повторно ініціалізувати систему:

- Витягнути всі модеми з HUB-ів
- Увімкнути проксі-сервер (Raidmax)
- Зачекати завантаження
- Підключити модем по одному з тайм-аутом 2 хвилини
- Перевірити адміністративну панель
- Якщо деякі з модемів не працюють - перевірити, чи є у них активний план.

В якості проксі-серверу запропоновано міні-комп'ютер Raspberry PI 3, який керує двома модемами (рис.9). Головна перевага Raspberry Pi - 40 контактів введення/виведення загального призначення (GPIO). До них можливо підключати периферію. Штатною операційною системою для Raspberry Pi є Linux. Вона встановлюється на microSD карту, а та – у спеціальний слот на платі.

Raspberry Pi 3 Model B має велику продуктивність і нові засоби комунікації *(Все про Raspberry Pi3. Botland. URL: https://botland.com.pl/399-raspberry-pi (дата звернення: 06.02. 2024))*:

- 64-бітний чотириядерний процесор ARM Cortex-A53 з тактовою частотою 1,2 ГГц на однокристальному чіпі Broadcom BCM2837;
- вбудований Wi-Fi 802.11n та Bluetooth 4.1.

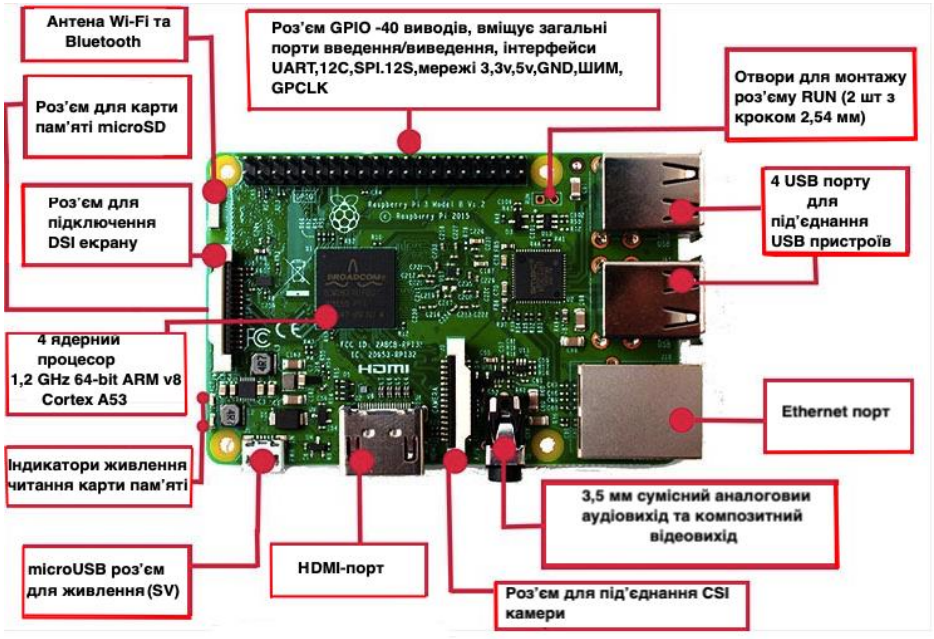


Рис.9- Конструкція Raspberry Pi 3 Model B

Крім того, процесор має архітектуру ARMv53, а значить, можливо використовувати операційні системи: Debian Wheezy, Ubuntu Mate, Fedora Remix і навіть MS Windows 10 IoT. Raspberry Pi 3 Model B має 1 ГБ оперативної пам'яті, але це пам'ять ділиться з графічної підсистемою. Графічний двоядерний процесор VideoCore IV® підтримує стандарти OpenGL ES 2.0, OpenVG, MPEG-2, VC-1 і здатний кодувати, декодувати та виводити Full HD-відео (1080p, 60 FPS, H.264 High-Profile).

Всі запити в системі відображаються за допомогою протоколу HTTP *(Захищений протокол HTTPS: що це таке, чим відрізняється від HTTP, як на нього перекласти сайт. Wedex. URL: https://is.gd/i9IPJT (дата звернення: 06.02. 2024)).*

Відповідно до специфікації OSI, HTTP відноситься до протоколів прикладного (верхнього, 7-го) рівня. Даний протокол передбачає використання клієнт- серверної структури передачі даних (рис.10).

Рис. 10- Клієнт-серверна структура передачі даних

На стороні клієнта формується запит і відправляється на сервер, після того як сервер приймає запит і успішно його опрацьовує, він одномоментно формує відповідь і повертає її зворотно, на сторону клієнта. Після цього клієнтський застосунок може надіслати інший запит, і процес “спілкування” відбудеться по аналогічному шляху. На сьогоднішній день саме завдяки протоколу HTTP відбувається взаємодія всесвітньої павутини. Варто зазначити, що даний протокол часто застосовується при передачі даних іншими протоколами, а саме протоколами прикладного рівня, таких як SOAP, XML-RPC та WebDAV.

В даному випадку прийнято говорити, що протокол HTTP використовується як “ транспорт ”. API, а також багато інших програмних продуктів передбачає використання

HTTP, для передачі інформації. Дані в такому випадку можуть мати будь – який формат, наприклад, XML або JSON. В основному, передача даних здійснюється через TCP/IP з'єднання. Дане програмне забезпечення використовує TCP-порт 80, вказаний порт зазвичай використовується зі сторони клієнта по замовчуванню, проте при необхідності він може бути змінений на будь-який інший.

Для відправлення HTTP – запиту, необхідно сформувати пошукову строку якій в свою чергу як мінімум потрібно задати один заголовок, а саме Host. Даний заголовок є обов'язковим і повинен бути присутнім в кожному запиті. Варто зазначити, що перевизначення доменного імені відбувається на стороні клієнта, і відповідно коли ми відкриваємо TCP-з'єднання, то завантажений сервер не має ніякої інформації про цей, яка саме адреса використовується для з'єднання.

Приклад HTTP запиту

Розглядаючи HTTP запит можна виокремити такі його частини:

- Метод: Дану складову запиту можна інтерпретувати як послідовність символів, окрім розділювачів та службових знаків, що визначає операцію, яку необхідно виконати. Розглядаючи специфікацію HTTP 1.1 можна зазначити, що існує необмежена кількість методів, які можна використати, проте переважно використовуються стандартні методи такі як:

1. GET – отримання даних
2. POST – надсилання даних
3. PUT – вставка, обновлення даних
4. DELETE – видалення даних

- URI (Uniform Resource Identifier) - шлях до конкретного ресурсу, над яким необхідно здійснити певну операцію, наприклад використання метода GET. Деякі запити можуть не відноситися до конкретного ресурсу, в такому випадку на місці URL, може знаходитися службовий символ "*". Прикладом цьому може послугувати запит, який безпосередньо адресується серверу, а не якомусь конкретному ресурсу

- Заголовки – це набір пар, ім'я та значення. В заголовках передається різноманітна інформація про службу, яка може містити тип кодування повідомлень, назву, а також версію браузера.

- Тіло повідомлення – власне, самі дані, які ми хочемо передати. Дані можуть варіюватися від html – сторінки, яку повертає сервер, до фотографій, які користувач, власне загружає в зворотному напрямку.

Відповідь сервера має наступну структуру:

```
HTTP/1.1 302 Moved Temporarily
Server: nginx
Date: Sat, 08 Mar 2014 22:29:53 GMT
Content-Type: text/html
Content-Length: 154
Connection: keep-alive
Keep-Alive: timeout=25
```

Код статусу – три цифри котрі визначають статус і результат поверненого запиту. Наприклад, коли ми використали запит GET і сервер успішно опрацював наш запит і повернув очікувану інформацію, код статусу в такому випадку – 200. В разі, коли сервер повідомляє, що такого ресурсу не існує – це код 404. В разі, якщо у клієнта недостатньо привілей для отримання того чи іншого ресурсу, код статусу – 403. Специфікація HTTP 1.1 визначає 40 різних кодів HTTP, а також допускається розширення протоколу і використання додаткових кодів станів.

Пояснення до коду стану (Reason Phrase) – пояснення до коду відповіді призначене для спрощеного розуміння людиною можливістю краще зрозуміти природу помилки. Дане пояснення може бути стандартним, або визначеним самими розробниками при створенні ресурсу.

Тіло відповіді: Для визначення закінчення використовується значення заголовка Content-Length (в даному випадку відповідь містить 7 виїмкових байтів: слово «Wisdom» і символ розриву рядків).

Сам по собі протокол HTTP не передбачає використання шифрування для передачі інформації. Проте для даного протоколу є досить популярним розширення, яке реалізує передачу інформації, за допомогою криптографічного протоколу SSL або TLS.

Дане розширення - HTTPS (HyperText Transfer Protocol Secure). Для конкретних з'єднань здебільшого прийнято використовувати TCP-порт 443. HTTPS передбачає захист даних від перехоплення, а також гарантує захист від можливих атак типу - man-in-the-middle, в ситуації, коли сертифікат верифікується на стороні клієнта, і при цьому приватний ключ сертифіката, не є скомпрометованим, користувач не використання непідписаного сертифіката і на комп'ютері користувача не були впроваджені сертифікати центру сертифікації зловмисника.

Графічна частина системи виконується за допомогою HTML *(HTML — мова розмітки гіпертексту. Портал знань. URL: http://www.znannya.org/?view=html (дата звернення: 07.02. 2024)).*

Мова для розмітки гіпертексту (HTML) призначена для розробки веб-сайтів та різноманітних додатків. HTML є нащадком SGML, яка в свою чергу була надто складна для пересічних людей. Виокремивши також каскадні таблиці стилів(CSS) та мову програмування JavaScript, можна зазначити, що дане тріо формує фундамент всесвітньої павутини.

Одними з вагомих переваг HTML можна відмітити простоту, яка була досягнута за рахунок використання структурних елементів, так званих дескрипторів, або ж тегів. Також це можливість форматування документа без посилання на засоби відображення.

Веб-браузери отримують HTML – документи з веб – сервера, або ж локального сховища вашого комп'ютера. HTML описує структуру веб-сторінки семантично та спочатку містить підказки для зовнішнього вигляду документа.

Елементи HTML - це складові HTML-сторінок. За допомогою HTML-конструкцій, зображення та інші об'єкти, такі як інтерактивні форми, можуть вбудовуватися у візуалізовану сторінку. HTML забезпечує засіб для створення структурованих документів, позначаючи структурну семантику для тексту, таких як: заголовки, абзаци, списки, посилання, цитати та інші елементи. Елементи HTML розмежовані тегами, написаними за допомогою кутових дужок. Такі теги, як <img /> та <input /> безпосередньо вводять вміст на сторінку. Інші теги, такі як <p> оточують і надають інформацію про текст документа, і можуть включати інші теги як під-елементи. Браузери не відображають теги HTML, але використовують їх для інтерпретації вмісту сторінки.

Для розгортання панелі управління необхідно застосовувати web-сервери. До функціоналу веб-сервера можна віднести виконання багатьох задач, таких як завантаження, а також резервне копіювання файлів в інтернеті через хмарні служби зберігання даних, або ж сервіси резервного копіювання, на випадок непередбачуваних ситуацій *(Що таке веб-сервер? FREEHOST.UA. URL: https://is.gd/1gNb6W (дата звернення: 07.02.2024)).*

Для розробки soft- частини застосовували мову програмування Python. Ця мова реалізує декілька парадигм програмування, включаючи об'єктно-орієнтовану, імперативну та функціональну. Має динамічну систему типів та прибиральника сміття. Однією із значних переваг Python є велика кількість відкритих і доступних бібліотек, практично в усіх галузях, котрі постійно доповнюються і розвиваються, за рахунок величезної спільноти.

Інтерпретатори Python доступні для установки на багатьох операційних системах, що дозволяє використовувати написані на ньому програми, в широкому спектрі систем.

В Python можна використовувати і інші парадигми, таких як design by contract та логічне програмування за допомогою зовнішніх розширень. Python використовує динамічне введення тексту та циклічний пошук прибиральника сміття для управління пам'яттю. Також однією із особливостей Python є пізнє зв'язування, котре пов'язує імена методів та змінних під час виконання програми. Дизайн Python надає змогу розробляти програми прогами в функціональному стилі, дотримуючись традицій Lisp *(Підручник з Python. Python. URL: https://docs.python.org/uk/3/tutorial/index.html, (дата звернення: 07.02. 2024)).*

Мова має вбудовані функції фільтрації, роботи з кортежами, списками, генераторами випадкових значень. Стандартна бібліотека має два модулі itertools та functools. Також Python має значні переваги перед різними мовами програмування:

- чистий синтаксис, дозволяє розбивати програму на окремі блоки та модулі;
- довільний стиль написання прогами (що характерно для більшості інтерпретованих мов);
- принцип роздільного створення модулів передбачає змогу використання тільки необхідних елементів і мінімальну кількість написаного коду;
- використання Python в інтерактивному режимі (дуже корисно для експериментів та вирішення простих проблем);
- наявність великої кількості бібліотек для візуалізації графічного інтерфейсу і даних;
- підходить для розв'язання математичних задач.

Окрім того, що Python це добре продумана і збалансована мова програмування, його активно використовують для реалізації в найрізноманітніших областях. Це може бути створення сценаріїв різних компонентів та реалізації автономних програм. Як мова загального призначення, Python розвивається в багатьох сферах від розробки веб-сайтів та ігор, до робототехніки та управління космічними кораблями. Програми Python можуть шукати файли та дерева каталогів, запускати інші програми, робити паралельну обробку процесів та ниток. Стандартна бібліотека Python оснащена прив'язками POSIX, розширення імен файлів, утиліти zip-файлів, аналізатори XML та JSON, обробники файлів CSV та інше. Крім того, основна частина системних інтерфейсів Python адаптовані для інтеграції; наприклад, сценарій, який зазвичай копіює дерева каталогів працює без змін на всіх основних платформах Python

Додатки розробляли з використанням фреймворку Flask *(Flask -посібник користувача. Project Links. URL: https://flask.palletsprojects.com/en/2.3.x/ (дата звернення: 07.02. 2024)).*

Flask це ліцензований BSD мікрофреймворк на основі Werkzeug та Jinja2.

Особливість мікрофреймворків, полягає в тому, що вони намагаються надати розробнику тільки необхідні компоненти для реалізації поставленої задачі. Мікрофрейморки можуть бути спеціально розроблені для створення APIs для певного сервісу, або сайту. Flask доволі простий, але одночасно і дуже гнучкий, що дає можливість розробникам використовувати тільки необхідні конфігурації, що полегшує розробку програм, або плагінів.

Два головні компоненти Flask це Werkzeug і Jinja2. Попри те, що Werkzeug несе відповідальність за надання маршрутизації, налагодження та інтерфейс шлюзу веб-сервера (WSGI), двигуном шаблону являється Jinja2.

Сам по собі, Flask не підтримує доступ до бази даних, автентифікацію користувачів чи будь-яку іншу утиліту високого рівня, але він реалізує підтримку великої кількості розширень, котрі реалізують вище перерахований функціонал. Простий додаток можна реалізувати навіть в одному файлі, проте при реалізації великого застосунку, краще розподілити програму на модулі. Модульна структура також один з переваг Flask. Сама ідея даного фреймворку полягає в реалізації надійної основи додатку, а функціонал верхнього рівня втілюють розширення.

Flask, як і всі інші бібліотеки Python, можна встановити, використовуючи індекси пакетів Python (PPI), його дуже просто налаштувати та почати розробляти.

Даний код імпортує бібліотеку Flask, ініціює додаток, створивши екземпляр класу Flask, оголошує маршрут, а потім визначає функцію для виконання при виклику маршруту.

```
from flask import Flask
app = Flask(__name__)

@app.route('/')
def hello_world():
    return 'Hello, From Flask!'

if __name__ == '__main__':
      app.run()
```

Цього коду достатньо для запуску першої програми Flask. Цей код запускає дуже простий вбудований сервер, котрий чудово підходить для тестування, але недостатньо потужний для введення додатку в експлуатацію. Flask не здійснює підтримку доступу до бази даних, і для здійснення взаємодії з БД, здебільшого використовують розширення Flask під назвою Flask-SQLAlchemy, що надає підтримку бібліотеки SQLAlchemy. По суті, SQLAlchemy - це набір інструментів Python SQL та Object Relational Mapper, що забезпечує розробникам повну потужність і гнучкість SQL. SQLAlchemy здійснює повну підтримку

парадигм дизайну на рівні підприємства та розроблена для високоефективного доступу до бази даних, зберігаючи ефективність та простоту використання. Хорошим тоном при розробці застосунку вважається, реалізація модуля аутентифікації користувача, CRUD (створення, читання, оновлення та видалення даних), API REST для створення, пошуку, маніпуляцій та видалення об'єктів. Також Flask надає змогу інтеграції утиліти Swagger для створення документації API, написання тестів та їхньої інтеграції. Для вузьконаправленого тестування функцій, прийнято використовувати pytest, який є повнофункціональним інструментом для тестування Python – застосунків. Pytest дозволяє легко розробляти тести, і все ж ця бібліотека достатньо масштабована для підтримки складних випадків використання. Postman, являється повноцінною платформою API REST, і надає інструменти інтеграції для кожного етапу життєвого циклу API, що робить розробку API простішою та надійнішою *(Огляд Proxy Seller. Affiliatebay. URL: https://www.affiliatebay.net/uk/proxyseller-review/ (дата звернення: 07.02. 2024)).*

Графічна бібліотека Folium застосовувалася ля розробки додатків. Folium - це потужна бібліотека Python, яка реалізовує декілька типів карт Leaflet. Той факт, що результати Folium є інтерактивними, робить цю бібліотеку дуже ефективною при побудові інформаційної панелі. Вона використовує механізм шаблонів Jinja2Python для візуалізації кінцевих результатів, а Pandas – відповідає за прив'язку статистичних даних CSV. Реалізація починається з імпорту, а потім відбувається визначення даних джерела. Folium реалізує міст між можливостями обробки даних Python та можливостями візуалізації інтерфейсу, які пропонує JavaScript. Зокрема, це дозволяє розробникам Python інтегрувати дані GeoJSON і ТороJSON з бібліотекою Leaflet, однією з найбагатших бібліотек, котру використовують на фронтенді для створення інтерактивних карт. Перевага використання такої бібліотеки, як Folium, полягає в тому, що вона безперебійно обробляє переклад між структурами даних Python та компонентами JavaScript, HTML та CSS.

До мінусів цієї бібліотеки можна віднести проблеми з відображенням карт, у випадку комбінації маркерів та спливаючих вікон, візуалізуючи велику кількість елементів. При рендерингу карти Folium, необхідно створити об’єкт самої карти, встановивши поряд координати центру карти, рівень масштабування карти, базової плитки для нашого фону.

Розглядаючи бібліотеку Folium, варто зазначити декілька речей *(Folium-бібліотека Python. Folium. URL: https://python-visualization.github.io/folium/ (дата звернення: 07.02.2024))*:

- Карта створена за допомогою даної бібліотеки визначаються як folium. Map object. Ми можемо додати інші об’єкти, поверх першого, таким чином реалізуючи

більш детально відображення і можливість додавати нові об'єкти.

- Бібліотека дозволяє власноруч створювати, або вибирати шаблони карт, наприклад, з OpenStreetMap, MapBox.

- Folium надає змогу вибирати різні проекції на карті. Доволі часто використовують сферичну проекцію Меркатора, особливо при візуалізації площі, порівняно невеликих розмірів.

Розглядаючи атрибути бібліотеки варто відмітити такий параметр як location, котрий задає точку фокусу на карті. Атрибут zoom_start дозволяє змінювати маштаб карти. Параметр control_scale, вимикає масштаб карти при певному, заданому рівні збільшення. Це те, що іноді може бути корисним для користувача, щоб отримати уявлення про масштаби географічної області, котру він переглядає.

Таким чином:

− Аналіз VPN та проксі-серверів показав, що найкращим підходом є використання змішаної моделі, яка комбінує переваги обох технологій. Це дозволить користувачам забезпечити високий рівень приватності, шифрування та анонімності завдяки VPN, а також використовувати проксі-сервери для додаткової прихованості їхньої реальної IP-адреси.

− Розроблена віртуальна приватна система повного циклу, що складається з наступних частин:

- Панель управління: розроблена за допомогою мови програмування Python та web-framework Flask. У якості веб - серверу була обрана модель Nginx + Werkzeug. Клієнтський інтерфейс був реалізований за допомогою шаблонізатора Jinja2. База данних - PostgreSQL, так як вона має гарну підтримку ORM у Python за допомогою бібліотеки SQLAlchemy.

- Головний сервер: містить в собі змішаний тип розробки. API частина була розроблена за допомогою Flask-RESTfull та мови програмування Python. Також були додані bash скрипти для контролю за підключеннями та управління Raspberry PI міні-комп'ютерами.

- На міні-комп'ютері Raspberry PI була встановлена операційна система (Raspbian). За допомогою bash скриптів та мови програмування Python було створено взаємозв'язок з модемами (Huawei e3372h). Реалізація маршрутизації пакетів була виконана за допомогою бібліотеки 3proxy. Реалізація VPN з'єднань мала змогу завдяки стандартній бібліотеці OpenVPN.

Запропонована SaaS (Software-as-a-Service) система має змогу надавати послуги як поодинокім користувачам, так і великим кампаніям. Продукт дозволяє отримувати доступ до заблокованих ресурсів та бути максимально анонімним користувачем для систем аналізу

трафіку. Також увесь трафік має шифрування, що дозволяє підвищити безпеку використання системи.

References:

Що таке VPN і яка його актуальність у наш час. ROOT NATIONAL, 2024. URL: https://is.gd/R4rG5W (дата звернення: 03.02.2024).
Посібник з VPN: що таке VPN-з'єднання та як воно працює? VPN WIKI. URL: https://is.gd/mygQrg (дата звернення: 03.02.2024).
Проксі-сервер: що це таке і чи потрібен він вам? Surfshark. URL: https://surfshark.com/uk/blog/proxy-server (дата звернення: 03.02.2024).
Yee C. K., Zolkipli M. F. Review on Confidentiality, Integrity and Availability in Information Security. // *Journal of ICT in Education.*- 2021.- Vol. 8.- P.34-42.
Технології забезпечення безпеки мережевої інфраструктури: підручник / В. Л. Бурячок та інш. Київ.: КУБГ, 2019. -218 с
Що таке VPN-підключення і як працює VPN? Самоосвіта URL: https://samoosvita.in.ua/scho-take-vpn-pidklyuchennya-i-yak-pratsyue-vpn (дата звернення: 05.02. 2024).
Що таке проксі-сервер. Hosting Ukraint. URL: https://is.gd/olaSI9 (дата звернення: 05.02. 2024).
Dsfferent Types if Proxy Servers and Their Uses. Securiwiser. URL: https://is.gd/J5ewRJ (дата звернення: 05.02. 2024).
Typical Proxy. Brightdata. URL: https://is.gd/8IbjQR (дата звернення: 06.02. 2024).
Все про Raspberry Pi3. Botland. URL: https://botland.com.pl/399-raspberry-pi (дата звернення: 06.02. 2024).
Захищений протокол HTTPS: що це таке, чим відрізняється від HTTP, як на нього перекласти сайт. Wedex. URL: https://is.gd/i9IPJT (дата звернення: 06.02. 2024).
HTML — мова розмітки гіпертексту. Портал знань. URL: http://www.znannya.org/?view=html (дата звернення: 07.02. 2024).
Що таке веб-сервер? FREEHOST.UA. URL: https://is.gd/1gNb6W (дата звернення: 07.02.2024).
Підручник з Python. Python.
URL: https://docs.python.org/uk/3/tutorial/index.html, (дата звернення: 07.02. 2024).
Flask -посібник користувача. Project Links.
URL: https://flask.palletsprojects.com/en/2.3.x/ (дата звернення: 07.02. 2024).
Огляд Proxy Seller. Affiliatebay. URL: https://www.affiliatebay.net/uk/proxyseller-review/ (дата звернення: 07.02. 2024).
Folium-бібліотека Python. Folium. URL: https://python-visualization.github.io/folium/ (дата звернення: 07.02.2024).

DOI 10.5281/zenodo.10822120

UDC 004.715

CHAPTER 22.
THE WIRELESS NETWORK "EASY NET EVERYWHERE" PRACTICAL IMPLEMENTATION

Volodymyr SMIRNOV

Assoc. Prof., PhD tech. sci.

Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

(8 Universytetskyi Ave, Kropyvnytskyi, Ukraine)

swckntu@gmail.com

https://orcid.org/0000-0002-4752-0527

Natalia SMIRNOVA

Assoc. Prof., PhD tech. sci.

Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

(8 Universytetskyi Ave, Kropyvnytskyi, Ukraine)

swckntu@gmail.com

https://orcid.org/0000-0002-5683-5766

Abstract. The results of the practical implementation of a 2.4 GHz wireless network for use in geographically distributed systems requiring wireless communication with control objects with guaranteed delivery of commands and data at a speed of 250 Kbps within a radius of up to 10 km are presented. The network characteristics, applications and limitations are presented. The network architecture, structure of network nodes, types of antennas used, and recommendations for selecting the optimal channel for network operation are described. The article describes the configuration of various networking models, their features and practical implementation.The network node addressing system for simple and cluster network models is described. The process of configuring, testing, and verifying the network's performance is described. An example of the location of network nodes on the ground and an example of data exchange in the network are presented.

Key words: wireless network, network node, antenna, cluster, controller, repeater, router, protocol.

ПРАКТИЧНА РЕАЛІЗАЦІЯ БЕЗПРОВІДНОЇ МЕРЕЖІ «EASY NET EVERYWHERE»

Анотація. Представлено результати практичної реалізації бездротової мережі діапазону 2.4 GHz для застосування в територіально-розподілених системах, що потребують наявності бездротового зв'язку з об'єктами управління з гарантованою доставкою команд і даних зі швидкістю 250 Kbps у радіусі до 10 км. Наведено характеристики мережі, сферу застосування та обмеження. Описано архітектуру мережі, структуру вузлів мережі, типи застосовуваних антен і рекомендації для вибору оптимального каналу для роботи мережі. Описано конфігурацію різних моделей побудови мережі, їхні особливості та практичну реалізацію. Описано систему адресації вузлів мережі для простої та кластерної моделі мережі. Описано процес конфігурування, тестування та перевірки працездатності мережі. Представлено приклад розміщення вузлів мережі на місцевості та приклад обміну даними в мережі.

Ключові слова: бездротова мережа, вузол мережі, антена, кластер, контролер, ретранслятор, роутер, протокол.

Вступ. На сьогодні розробка та реалізація бездротових мережевих технологій, мереж, систем і пристроїв для керування віддаленими та розподіленими в просторі об'єктами є актуальним завданням.

Такі системи та мережі повинні відповідати вимогам надійності, стійкості до перешкод, скритності в роботі, мати високий поріг виявлення, а також володіти достатнім рівнем захисту надісланих команд і даних.

Авторами в рамках науково-дослідної теми «Створення мобільної мережі 2.4 GHz з адаптивною аморфною топологією для управління роєм БПЛА і робототехнічних об'єктів», реєстраційний № 0120U104088, було проведено аналіз наявних бездротових мереж на предмет їхньої відповідності зазначеним вимогам.

Аналіз показав, що за сукупністю характеристик аналізовані мережі, такі, як:

- ZigBee *(IEEE 802.15.4-2020 - IEEE Standard for Low-Rate Wireless Networks,2020);*
- Z-Wave *(Recommendation G.9959,2013)*;
- LoRaWan *(LoRaWAN™ Specification,2015)*

не здатні повною мірою вирішувати поставлені задачі.

На підставі результатів аналізу, авторами були проведені дослідницькі та дослідно-конструкторські роботи (ДКР), які дали можливість розробити:

- архітектуру *(Смирнов В.В., Смирнова Н.В. Архитектура контроллера узла адаптивной мобильной сети с аморфной топологией,2020),*

- систему протоколів *(Смирнов В.В., Смирнова Н.В. Архітектура адаптивної бездротової локальної мережі для управління об'єктами і пристроями,2020)*,

- програмне і апаратне забезпечення *(Смирнов В.В., Смирнова Н.В.Бездротова локальна мережа класу Smart Home на базі модулів сплітерів-репітерів,2021)* бездротової мережі.

Мережа має можливість швидкого розгортання, властивість масштабування, а також здатність зміни топології без негативного впливу на роботу всієї мережі.

Розроблена мережа не використовує протоколи стека TCP/IP, що дало змогу значно скоротити розмір службової інформації в переданих пакетах, що підвищило поріг виявлення вузлів, які працюють у мережі *(Смірнов В.В., Смірнова Н.В. Мобільна mesh-мережа для управління роєм об'єктів,2023).*

Розроблені авторами мережеві протоколи дають змогу вузлам мережі здійснювати сеанси обміну даними в умовах, коли діапазон частот, що використовується, "зашумлений" іншими пристроями, що працюють у тому самому діапазоні.

У монографії представлено практичну реалізацію одного з напрямів науково-дослідної теми № 0120U104088, а саме: бездротової локальної мережі під назвою «Easy Net Everywhere».

1. Призначення та область застосування мережі

Призначення

Бездротова мережа "Easy Net Everywhere" призначена для застосування в територіально-розподілених системах, які потребують наявності бездротового зв'язку з об'єктами управління з гарантованою доставкою команд і даних зі швидкістю 250 Kbps у радіусі до 10 км (залежно від умов навколишньої місцевості та складу обладнання).

Область застосування

Мережа "Easy Net Everywhere" може бути використана для вирішення завдань у проектах різного ступеня складності, наприклад:

- для управління як окремими об'єктами, так і роєм об'єктів, наприклад, дронами, роботами, роботизованими платформами та іншими механізмами;
- для використання в якості фреймворку для побудови різних систем і реалізації проектів рівня "Internet Of Things";
- для отримання і пересилання в мережу координат GPS, створення GPS трекерів і маячків тощо;
- для віддаленого керування станом об'єктів у комунальних службах, наприклад, водопровідними засувками, кранами, клапанами тощо;

- для збирання та передавання інформації з віддалених автономних датчиків, датчиків пристроїв автоматики, медичних приладів тощо;
- для систем керування дозаторами, зерносушарками, теплицями тощо;
- для систем автоматичного керування мікрокліматом, поливом, освітленням тощо;
- для систем керування міськими світлофорами з метою підвищення комфорту пересування автомобільного транспорту, зниження рівня ДТП тощо;
- для систем управління класу "Smart Home», увімкнення/вимкнення побутових приладів і електроприводів, для управління потужністю в навантаженні тощо;
- для швидкої реалізації територіально-розподілених DIY-проектів (Arduino тощо) ;
- для створення текстових месенджерів і чатів.

Область застосування мережі обмежується тільки її технічними характеристиками.

Технічні характеристики:

Частотний діапазон: ISM.

Радіоканали: 0-125 (від 2400 до 2525 МГц).

Полоса пропускання радіоканалу - 1МГц.

Трансивери: NRF24L01+, NRF24L01+PA+LNA, E01-ML01DP5, E01-2G4M27D.

Відстань приймання/передавання даних у межах прямої видимості на висоті 1 м на швидкості 250 Kbps:

- трансивер NRF24L01 - 100 м;
- трансивер NRF24L01+PA+LNA, E01-ML01DP5 - 1км;
- трансивер E01-2G4M27D - 2 км.

Швидкість передачі даних: 250 Kbps, 1 Mbps і 2 Mbps.

Максимальна довжина пакета: 256 байт.

Час передачі пакета 256 байт на швидкості 250 Kbps - 50 мс (5 Кб/с).

Інтерфейси користувача:

- UART 9600 - 921600 baud;
- Bluetooth: BLE.

Інтерфейси контролера мережі:

- I^2C;
- SPI;
- GPS UART 115200 baud.

Кількість функціональних виводів контролера – 14.

Функції виводів контролера (призначаються користувачем):

- ADC - 14;
- DAC - 2;
- PWM - 11;
- Servo - 11;
- GPIO: вихід - 11, вхід - 14, input only - 3;
- GPIO переривання – 14.

Архітектури мережі:

Архітектура "багато-до-багатьох":

- кількість вузлів – 254.

Кластерна архітектура:

- кластерів - 14;
- кількість вузлів у кластері - 15;
- кількість роутерів - 30.

Напруга живлення: 3,3 В, 5 В.

Струм споживання вузла мережі:

- в активному режимі: 40 ма;
- у пасивному режимі: 25 мка.

Діапазон робочих температур: -40ºС...+85ºС.

Особливості мережі

Мережа "Easy Net Everywhere" має кластерну архітектуру з маршрутизацією пакетів і можливістю масштабування.

Вузлами мережі використовуються трансивери невеликої потужності для забезпечення обміну даними тільки там, де це необхідно, не займаючи ефір там, де це небажано.

Таке рішення забезпечує створення оптимальної топології мережі, підвищення порога виявлення роботи трансиверів і зменшення ймовірності виникнення колізій. Розв'язання колізій у мережі реалізується пропрієтарним протоколом.

Вузли мережі можуть одночасно працювати як у режимі точка-точка на невеликій дистанції в межах прямої видимості до 2 км, так і в режимі ретрансляції пакетів, що дає можливість встановлювати зв'язок між об'єктами на відстані до 10 км, а через мережу StarLink, мережу GSM і GSM-Internet - у встановлених межах.

Передавання даних здійснюється каналами, які обираються випадковим чином із числа доступних. Теоретично доступно 125 каналів з шириною смуги пропускання 1 МГц. Практично - залежить від конкретних умов.

Усі вузли мережі рівнозначні і можуть мати повний або обмежений доступ до інших вузлів мережі залежно від використаної архітектури.

Кожен вузол мережі може передати команди і дані будь-якому іншому вузлу.

Адміністратор мережі може встановити необхідні обмеження для кожного вузла. Адміністрування мережі можливе з будь-якого вузла, наділеного повноваженнями.

Кожна наступна транзакція не використовує повторно канал попередньої транзакції, що ускладнює виявлення вузла сканерами ефіру. Тривалість однієї транзакції на одному каналі не перевищує 25 мс.

Девіація каналів передавання даних може бути встановлена адміністратором у межах +/- 2...60 від частоти основного каналу.

Адміністратор може встановити обмежений список робочих каналів, при цьому кожному адресату може бути поставлено у відповідність один або кілька фіксованих/змінних каналів.

Безпека. Кожен вузол мережі має адресу мережі, адресу вузла, пароль і логін мережі, а також пароль доступу до вузла через Bluetooth.

Шифрування даних: пропрієтарний алгоритм маскування даних.

Передача даних у мережі може ініціюватися:

- користувачем;
- вузлом мережі;
- подією;
- перевищенням/зниженням значення параметра відносно заданого порога;
- після закінчення часу таймера одноразово або із заданою періодичністю.

Для передавання даних вузлу-одержувачу використовується маршрутизація відправника. Для кожного вузла-одержувача можна вказати свій маршрут проходження пакетів і записати його в профіль адресата.

Така маршрутизація детермінована і для стаціонарних і малорухомих об'єктів оптимальніша, ніж стохастична маршрутизація в mesh-мережі.

Взаємодія користувача з будь-яким вузлом мережі здійснюється за допомогою послідовного інтерфейсу UART на швидкості до 921600 baud або за допомогою інтерфейсу Bluetooth (BLE).

Конфігурація та встановлення параметрів вузлів мережі здійснюється за допомогою АТ- команд через бездротовий інтерфейс Bluetooth (BLE) планшета або смартфона та дротовий інтерфейс UART.

Усі налаштування зберігаються в пам'яті вузла.

Обмеження:

- обмеження 1 зумовлене частотою роботи трансивера - 2.4 GHz. Зв'язок можливий у межах прямої видимості;
- обмеження 2: за надто великої дистанції між роутерами зв'язок на даній ділянці може перерватися і мережа розпадеться на кілька самостійних сегментів.

Для виключення такої ситуації кількість роутерів на одиницю площі/обсягу ареалу функціонування мережі має бути більшою за мінімально необхідну кількість. У цьому разі існує більше варіантів вибору альтернативних маршрутів проходження пакетів.

2. Опис компонентів і вузлів мережі

Трансивери

У всіх вузлах мережі передбачено використання трансиверів різної потужності залежно від розв'язуваних завдань. Трансивер вузла вибирається користувачем. Трансивер або впаюється в плату вузла (рекомендується), або вставляється в роз'єм (для тестування).

Вузли мережі працюють із такими трансиверами:

- трансивери NRF24L01+, NRF24L01+PA+LNA (рис.1);
- трансивери E01-ML01DP5, E01-2G4M27D (рис.2).

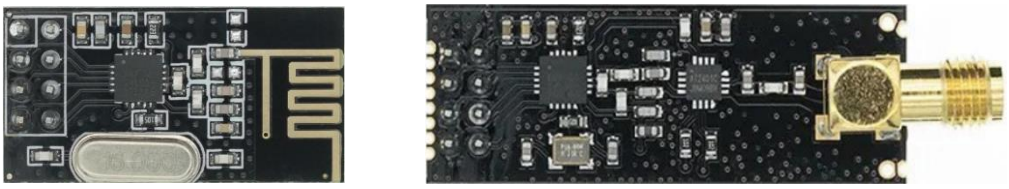


Рисунок 1 - Трансивери NRF24L01+ та NRF24L01+PA+LNA

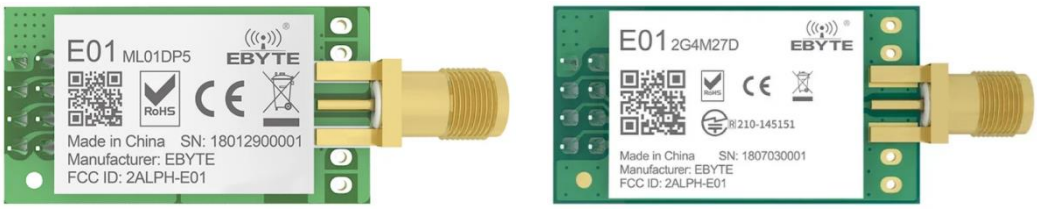


Рисунок 2 – Трансивери E01-ML01DP5 та E01-2G4M27D

Антени

З трансиверами можуть використовуватися різні антени, як штатні, так і спеціальні, з конектором SMA. Від вибору антени залежить відстань, на якій трансивери можуть забезпечити надійний зв'язок.

Штатна антена має коефіцієнт посилення 3 dBi і забезпечує впевнений зв'язок на відстані 1-2 км на відкритій місцевості на висоті 1,5 м з трансивером E01-2G4M27D (рис. 3).

Рисунок 3 - Штатна антена трансивера

Антена Yagi 10 dBi забезпечує впевнений зв'язок на відстані до 5 км на відкритій місцевості на висоті 1,5 м з трансивером E01-2G4M27D (рис. 4).

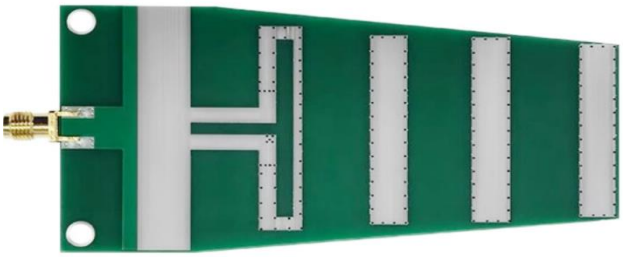


Рисунок 4 - Антена Yagi 10 dBi

Антена Yagi 25 dBi забезпечує впевнений зв'язок на відстані до 30 км на відкритій місцевості на висоті 1,5 м з трансивером E01-2G4M27D (рис. 5).

Рисунок 5 - Антена Yagi 25 dBi

Під час вибору антени слід враховувати діаграму спрямованості, яка вказується в технічних характеристиках конкретних антен.

Керування трансиверами здійснюється мікроконтролером ESP32 фірми Espressif, у керуючій програмі якого реалізовано стек системних, мережевих і користувацьких протоколів. Сукупність контролера і трансивера утворює вузол мережі.

Вибір оптимальних каналів для роботи мережі

Діапазон частот, у якому працює мережа, зумовлює певні вимоги до антен, що використовуються і вибору оптимального каналу (групи каналів) для роботи вузлів мережі.

Антени повинна мати мінімальне значення коефіцієнта стоячої хвилі КСВ (*SWR standing wave ratio*) в обраному діапазоні частот. Цей параметр визначає ККД антени і безпосередньо впливає на дальність зв'язку. Хвильовий опір антен для трансиверів становить 50 Ом.

Для визначення КСВ антен використовуються спеціальні прилади: КСВ-метри. Наприклад, у польових умовах для вимірювання необхідних параметрів антен можна використовувати LiteVNA (Potrable Vector Network Analizer).

Результати вимірювання КСВ штатної антени трансивера (рис. 3) за допомогою приладу LiteVNA представлені на рис. 6.

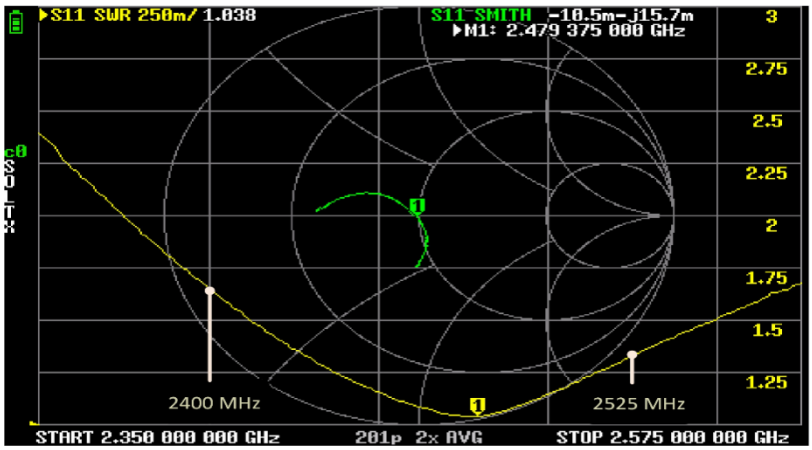


Рисунок 6 - Результати вимірювання КСВ штатної антени трансивера

З графіка випливає, що антена не є широкосмуговою. Мінімальний КСВ антени 1.038 відповідає частоті 2479 MHz або каналу з номером 79.

Прийнятний КСВ відповідає частотам 2450 MHz - 2500 MHz. Це означає, що основний канал для роботи мережі бажано вибирати в діапазоні від 50 до 100.

На рисунку 7 представлено скріншот екрана аналізатора TSA ULTRA (Tiny Spectrum Analyzer) з результатами сканування частот у діапазоні роботи мережі 2400 MHz - 2525 MHz (канали 0 - 125) під час виконання тесту для двох вузлів мережі.

На скріншоті відображено частоти, на яких здійснюється обмін даними між бездротовими пристроями:

- у діапазоні частот 2400 MHz - 2400 MHz працюють пристрої Wi-Fi;
- у діапазоні частот 2400 MHz - 2400 MHz працюють вузли мережі, займаючи канали 58 – 68;
- частота 2485 MHz відповідає основному каналу з номером 85.

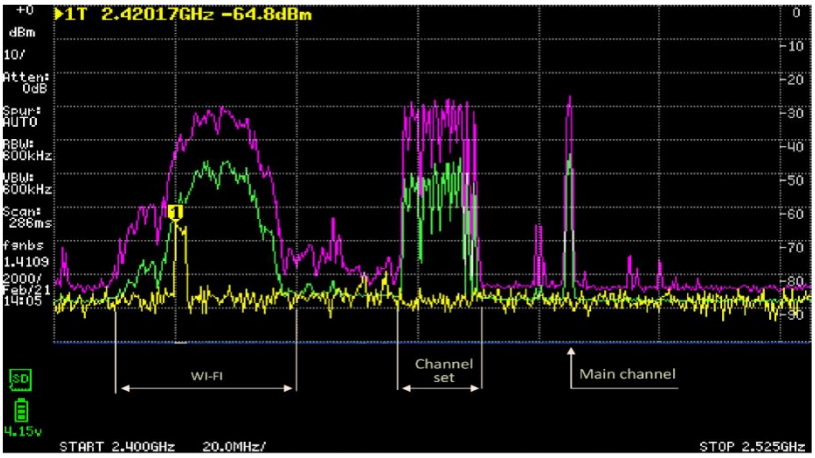


Рисунок 7 - Результат сканування діапазона 2400 MHz - 2525 MHz

Таким чином, знаючи КСВ антени, можна вибрати найбільш оптимальний діапазон частот (каналів) для роботи мережі.

У разі відсутності приладу для вимірювання КСВ антени, рекомендується обирати канали в середині робочого діапазону ISM і надалі коригувати їх на підставі статистичної інформації про помилки передавання даних за всіма обраними каналами (AT- команда *AT+ERROR.log*).

Призначення та структура вузлів мережі

Вузли мережі

Для побудови та організації роботи мережі використовуються мережеві функціональні вузли:

- "Net Master" (NM);
- "Controller" (C);
- "Light Node" (L);
- "Cluster Admin" (CA);
- "Net Router" (NR);
- "Repeater" (R).

Net Master. Вузол "Net Master" є головним об'єктом мережі та призначений для адміністрування мережі, надсилання команд і даних у мережу та отримання даних із мережі. Взаємодіє з мережею Internet за допомогою Wi-Fi роутера, за допомогою роутера Starlink і GSM-модема, що має підключення до UART.

Структурну схему вузла "Net Master" наведено на рис. 8.

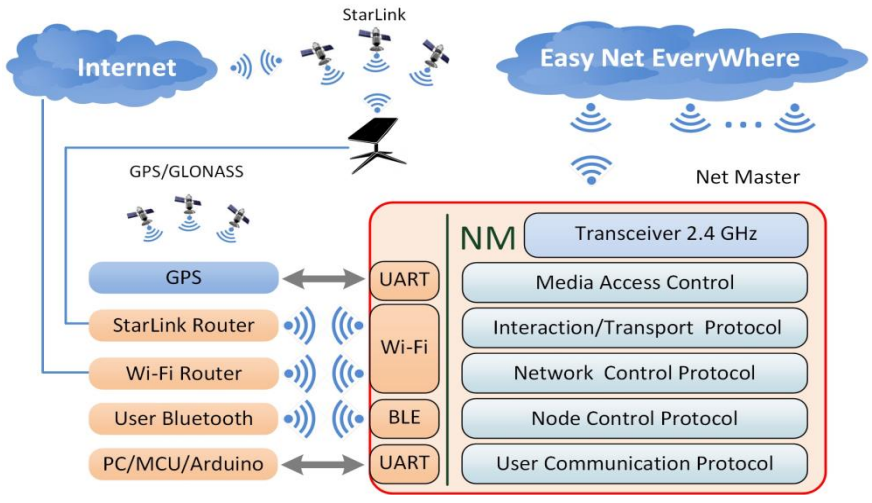


Рисунок 8 - Структурна схема вузла "Net Master"

Controller. Вузол "Controller" призначений:

- для приймання з мережі та передавання в UART команд і даних користувача, включно з текстовими повідомленнями довжиною до 256 байт;
- для виконання команд користувача;

- для збирання та передавання інформації.

Команди користувача являють собою числові значення, яким поставлено у відповідність виконання однієї дії на стороні контролера або послідовності дій, наприклад:

- увімкнути/вимкнути будь-який пристрій;
- збільшити/зменшити потужність у навантаженні;
- повернути вал одного або декількох сервоприводів на заданий кут з заданою швидкістю;
- встановити на виводах DAC рівень постійної напруги;
- прочитати поточне значення напруги на виводах ADC і передати їх користувачеві;
- встановити тайм-аут таймера для періодичного передавання користувачеві станів виводів і значень ADC тощо.

Вузол "Controller" має можливість підключення модуля GPS. Це дає змогу в реальному масштабі часу визначати координати кожного вузла мережі в просторі, передавати координати вузлу "Net Master" з подальшим відображенням їх на Google-карті (візуалізація топології мережі на смартфоні/планшеті або комп'ютері).

Це дуже корисна можливість для завдання оптимального маршруту проходження пакетів, відображення координат об'єктів, встановлення маячків, GPS-GSM трекерів, навігації дронів, роботизованих платформ тощо.

Структурна схема вузла "Controller" представлена на рис. 9.

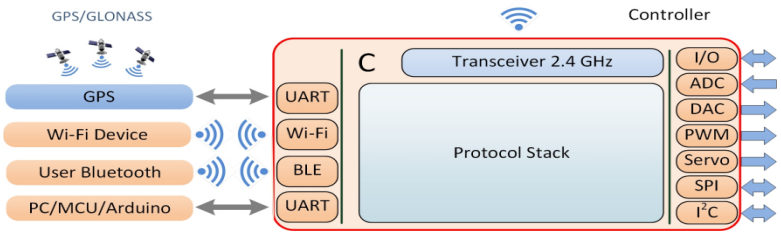


Рисунок 9 - Структурна схема вузла "Controller"

На структурній схемі вузла " Controller" з лівого боку представлені комунікаційні інтерфейси UART і Bluetooth для взаємодії користувача з контролером мережі.

З правого боку представлені послідовні системні інтерфейси SPI, I2C, і модулі контролера для управління обладнанням і отримання зовнішніх сигналів.

Light Node. Вузол "Light Node" призначений для двостороннього обміну командами і даними між інтерфейсом UART і мережею зі швидкістю до 921600 baud. Вузол не містить функціональних виводів. Для взаємодії з користувачем вузол "Light Node" має інтерфейси UART, Wi-Fi і Bluetooth (BLE).

Структурну схему вузла "Light Node" представлено на рис.10.

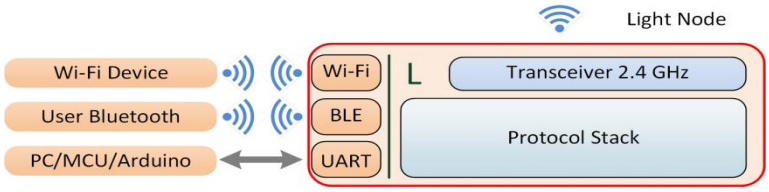


Рисунок 10 - Структурна схема вузла "Light Node"

Cluster Admin. Вузол "Cluster Admin" призначений для двостороннього обміну командами і даними користувача між інтерфейсом UART і мережею зі швидкістю до 921600 baud. Вузол здійснює адміністрування всіх вузлів кластера, виконує системні та сервісні функції для забезпечення роботи кластера. Для взаємодії з користувачем вузол "Cluster Admin" має інтерфейси UART і Bluetooth (BLE).

Структурну схему вузла "Cluster Admin" наведено на рис. 11.

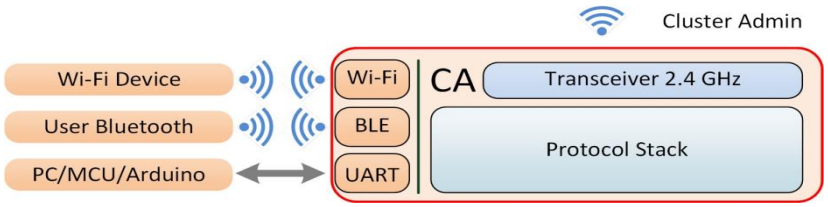


Рисунок 11 - Структурна схема вузла "Cluster Admin"

Net Router. Вузол "Net Router" призначений для маршрутизації пакетів у мережі відповідно до встановленого маршруту. Звільняє інші вузли мережі від участі в процесі маршрутизації та ретрансляції пакетів.

Реалізація вузла "Net Router" має два варіанти: одиночний і здвоєний. Одиночний роутер спочатку приймає дейтаграму, а потім передає. Оскільки режим роботи роутера симплексний, то під час передачі даних приймання даних не здійснюється. Загальний час прийому-передачі дейтаграми становить 50 мс.

У здвоєному роутері /“Fast Router”/ один роутер приймає дейтаграму, потім по інтерфейсу UART пересилає її другому роутеру, який передає дейтаграму в мережу. Час прийому-передачі дейтаграми становить 27 мс.

Для взаємодії з користувачем вузол "Net Router" має інтерфейси UART і Bluetooth (BLE).

Структурну схему одиночного вузла "Net Router" представлено на рис. 12.

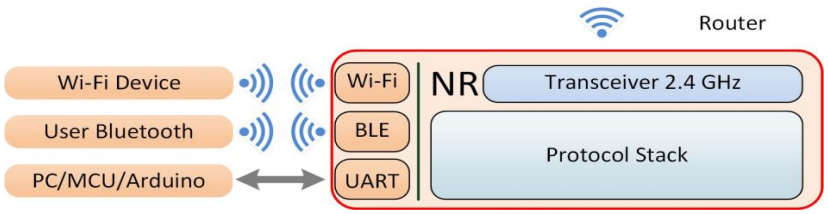


Рисунок 12 - Структурна схема одиночного вузла "Net Router"

Здвоєний роутер має дві мережеві адреси та по два інтерфейси UART і Bluetooth (BLE).

Структурна схема здвоєного вузла "Net Router" подана на рис. 13.

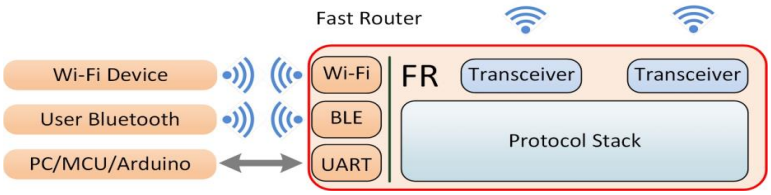


Рисунок 13 - Структурна схема здвоєного вузла "Net Router"

Repeater. Вузол "Repeater" (ретранслятор) призначений для локального розширення зони покриття мережі. Він є повільним пристроєм зі швидкістю передачі 2400 baud. Діапазон частот роботи репітера - 144 і 433 MHz.

Вузол "Repeater" доцільно використовувати в умовах поганого проходження сигналу 2,4 GHz або у відсутності можливості використання вузла "Net Router".

Вузол "Repeater" приймає і передає дейтаграму цілком по інтерфейсу UART під управлінням спеціального протоколу.

Структурну схему вузла "Repeater" наведено на рис. 14.

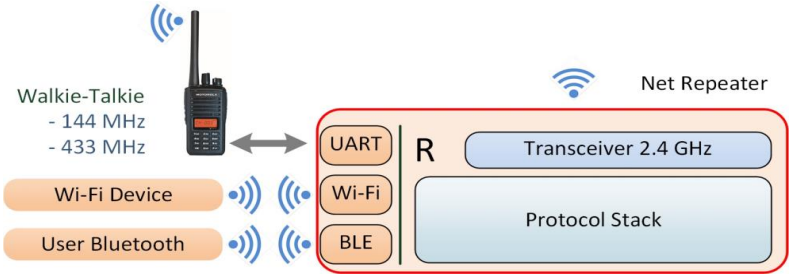


Рисунок 14 - Структурна схема вузла "Repeater"

2. АРХІТЕКТУРА, МАСШТАБУВАННЯ, АДРЕСАЦІЯ ТА РОБОТА МЕРЕЖІ

Архітектура мережі "Easy Net Everywhere" дає змогу користувачеві легко будувати необхідну топологію, оптимально відповідну для вирішення конкретного завдання.

У загальному вигляді архітектура мережі "Easy Net Everywhere" представлена на рис. 15.

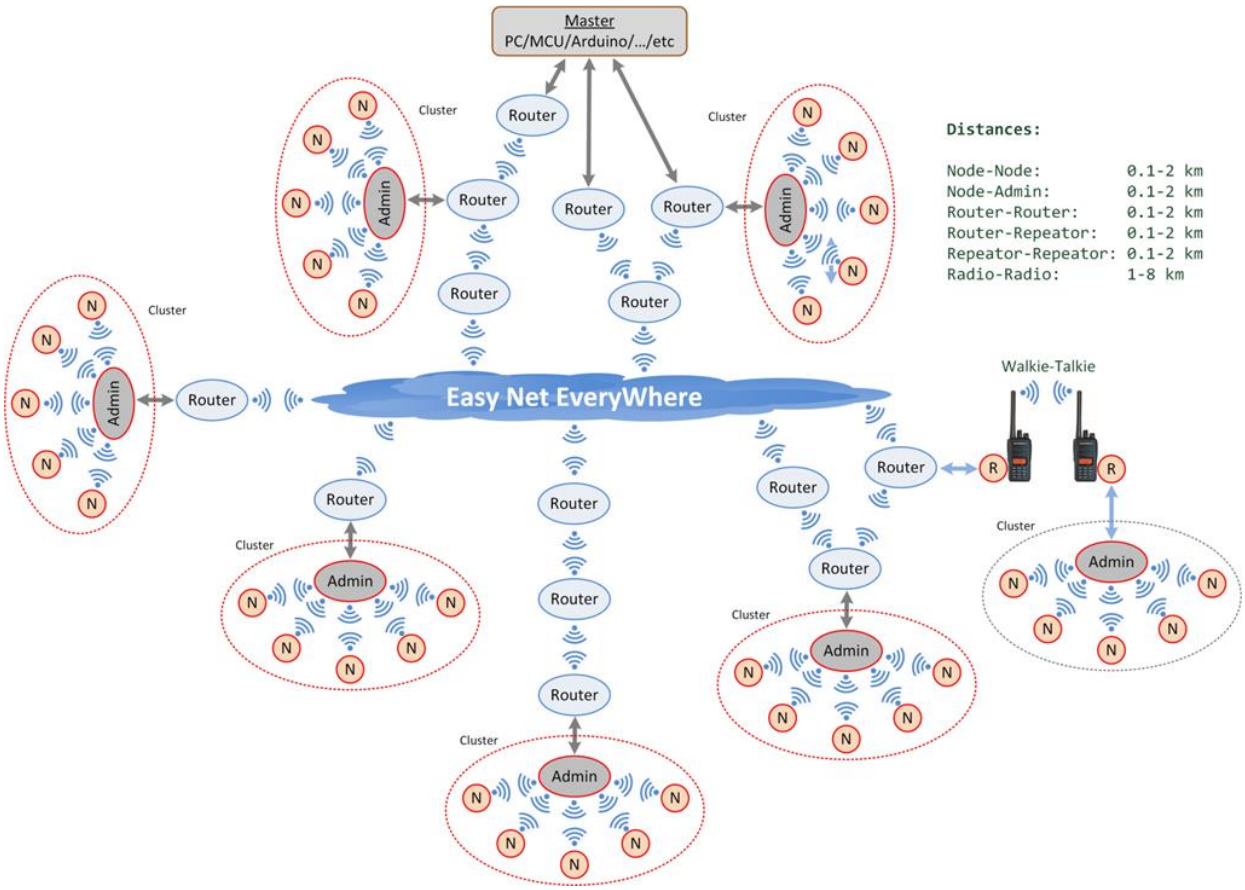


Рисунок 15 - Архітектура мережі "Easy Net Everywhere"

Масштабування мережі

Архітектура мережі "Easy Net Everywhere" є легко масштабованою.

Наприклад, для побудови системи "Розумний дім", що містить невелику кількість вузлів на невеликій площі за умов низького трафіку, застосування роутерів і репітерів недоцільне.

Однак, у територіально розподіленій системі з безліччю вузлів і відстанями між вузлами до 10 км, роутери та репітери є необхідністю.

Масштабування мережі реалізується відповідно до таких моделей:

- Модель "Simple Net";
- Модель "Light Cluster Net";
- Модель "Medium Cluster Net";
- Модель "Union Cluster Net".

Модель мережі "Simple Net" встановлює режим роботи простої мережі з аморфною архітектурою та аморфною топологією без використання роутерів та інших вузлів. У цьому режимі користувач і кожен вузол має прямий доступ до всіх інших вузлів мережі. Усі вузли за замовчуванням рівнозначні. За замовчуванням, Майстром мережі може стати будь-який вузол,

до якого в цей момент підключився користувач. Тому мережа може мати кілька Майстрів мережі, якщо це не заборонено адміністратором.

Така модель рекомендується для створення дуже малих локальних мереж з невеликим трафіком.

Архітектура мережі на основі моделі "Simple Net" представлена на рис. 16.

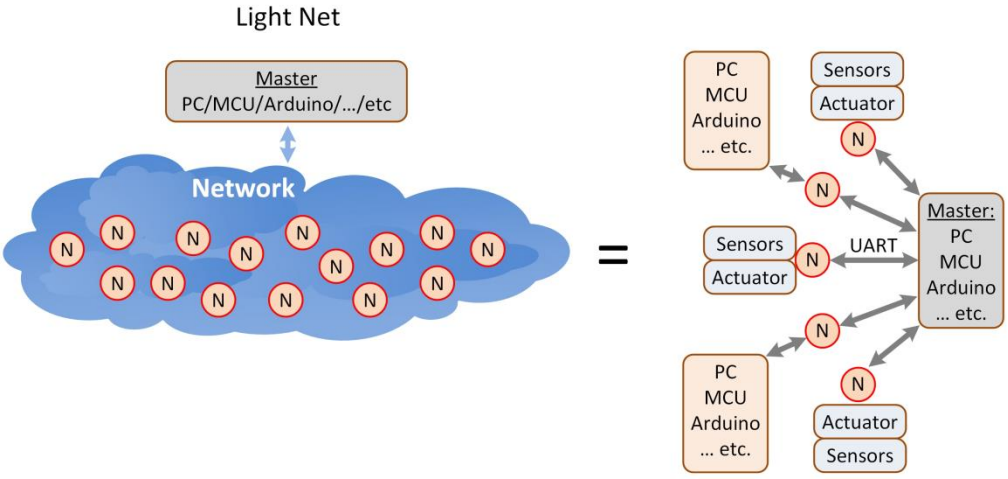


Рисунок 16 - Архітектура мережі на основі моделі "Simple Net"

Фізична реалізація мережі "Simple Net" представлена на рис. 17.

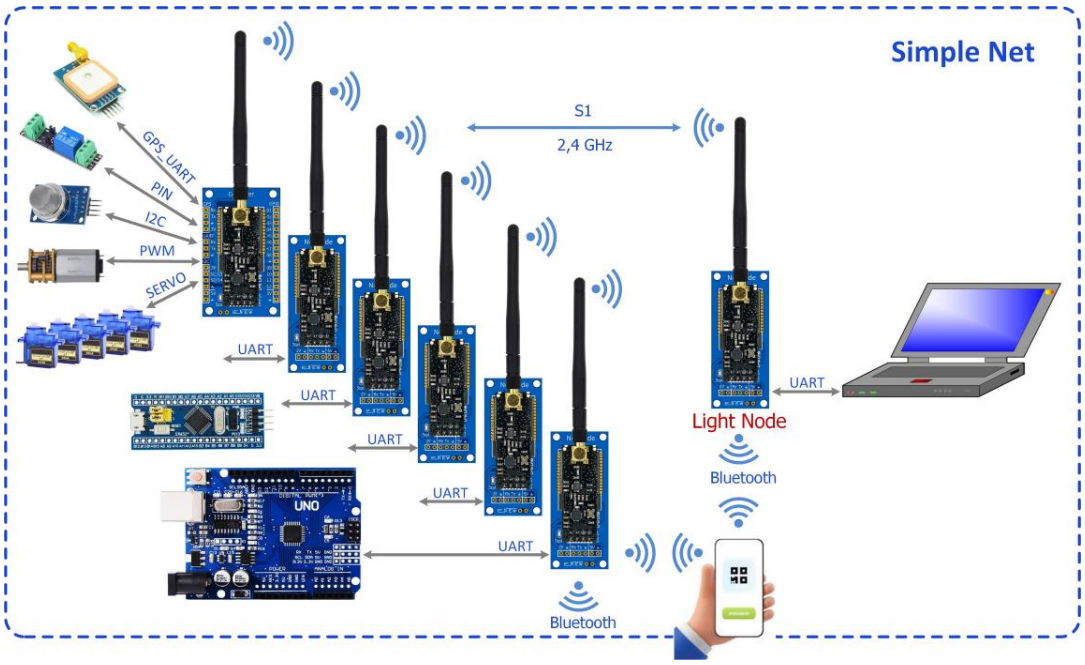


Рисунок 17 - Фізична реалізація мережі "Simple Net"

Значення дистанції S1 залежить від використовуваного трансивера та антени. Наприклад, у разі використання штатної антени і трансивера NRF24L01+PA+LNA дистанція S1 становить 1 км, а в разі використання трансивера E01-2G4M27D - 2 км.

Модель мережі "Light Cluster Net" встановлює режим роботи мережі з одним або кількома кластерами без використання роутерів. У цьому режимі доступ до вузлів кластера

здійснюється через вузол "Cluster Admin", який інкапсулює вузли кластера і звільняє користувача від роботи з управління вузлами "Light Node".

Вузли "Cluster Admin" мають прямий зв'язок із вузлом "Net Master" за інтерфейсом UART зі швидкістю до 921600 baud.

Така модель рекомендується для створення невеликих локальних мереж з невеликим трафіком.

Архітектура мережі на основі моделі "Light Cluster Net" представлена на рис. 18.

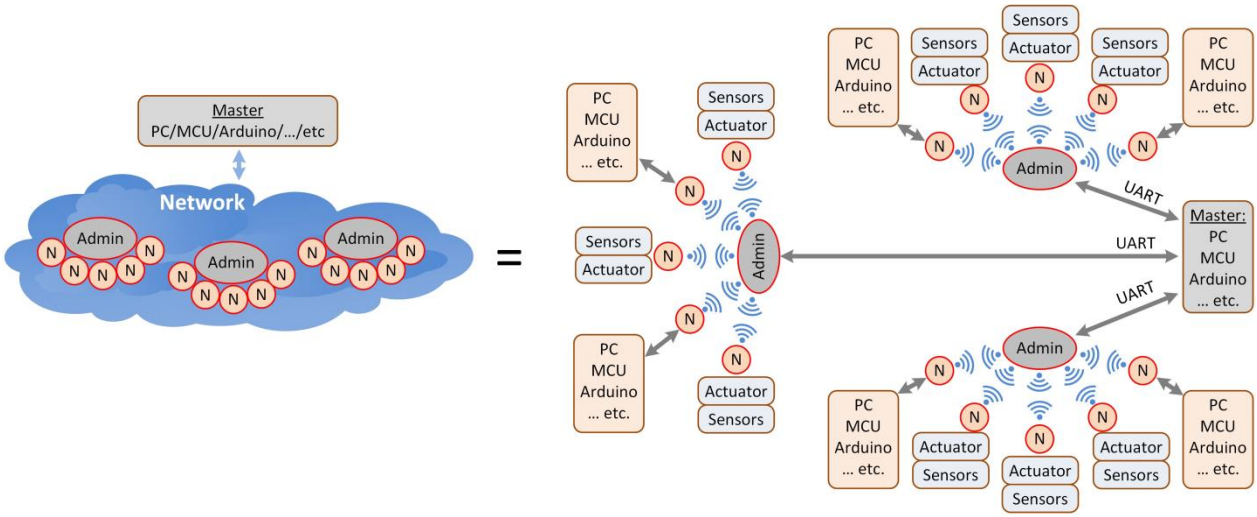


Рисунок 18 - Архітектура мережі на основі моделі "Light Cluster Net"

Фізична реалізація кластера мережі "Light Cluster Net" представлена на рис. 19.

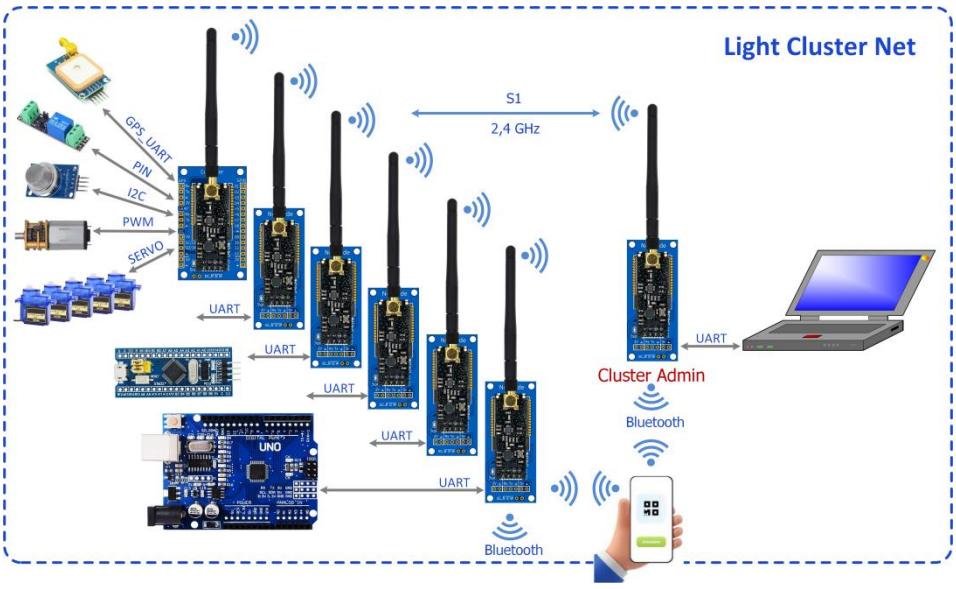


Рисунок 19 - Фізична реалізація кластера мережі "Light Cluster Net"

Модель "Medium Cluster Net" встановлює режим роботи мережі з декількома кластерами з використанням роутерів і репітерів та відносно високим трафіком в умовах наявності перешкод для проходження мережевих пакетів.

Доступ до вузлів мережі також здійснюється через вузол "Cluster Admin".

Така модель рекомендується для створення територіально-розподілених мереж з відносно високим трафіком. Фізична реалізація кластера мережі "Medium Cluster Net" представлена на рис. 20.

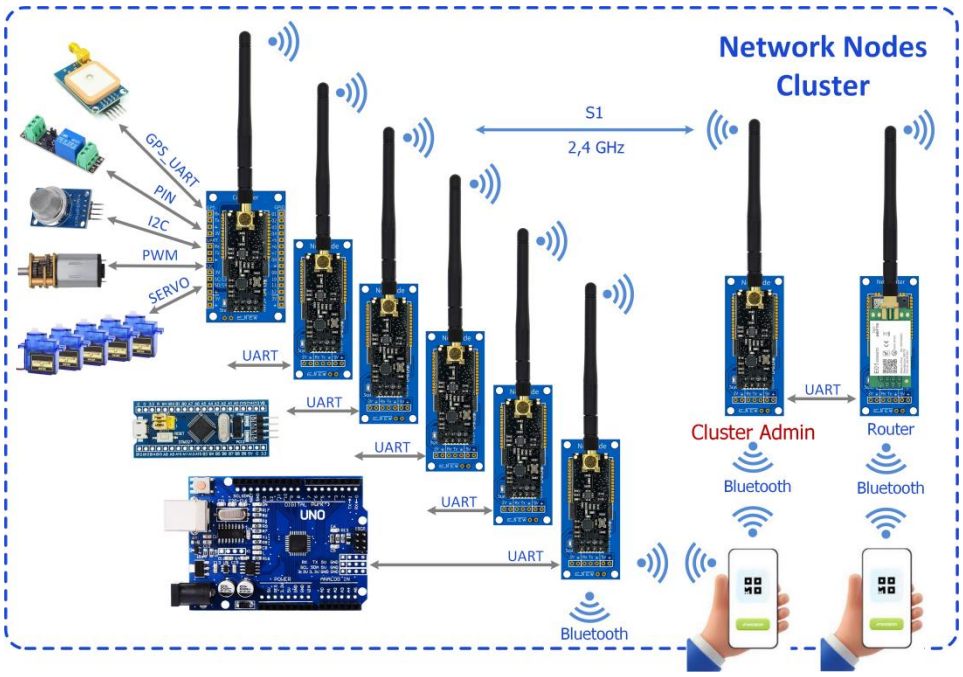


Рисунок 20 - Фізична реалізація кластера мережі "Medium Cluster Net"

Архітектура мережі на основі моделі "Medium Cluster Net" представлена на рис. 21.

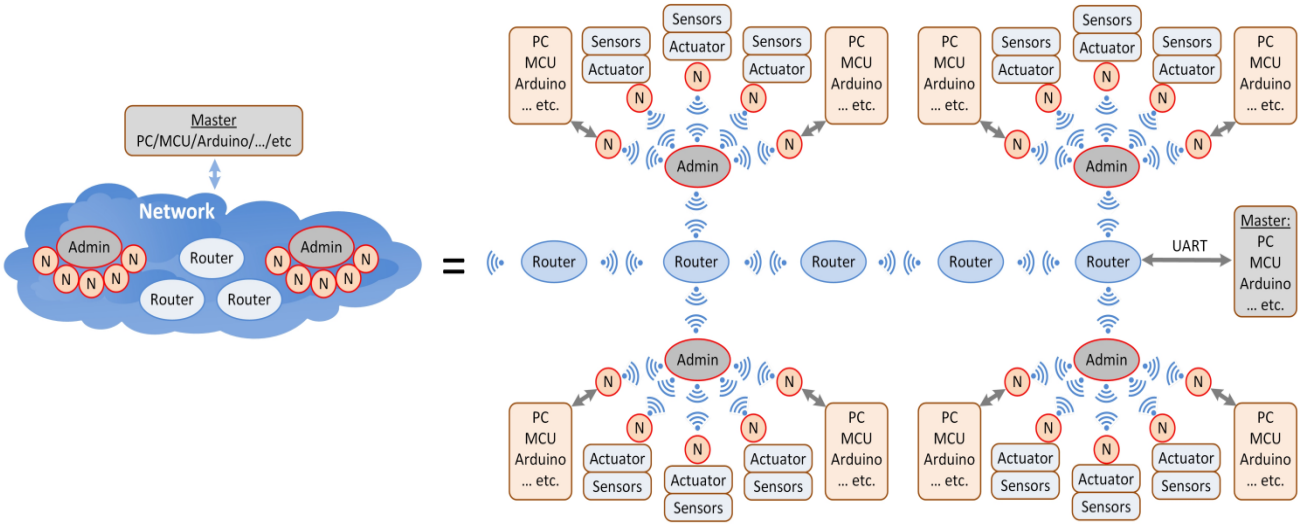


Рисунок 21 - Архітектура мережі на основі моделі "Medium Cluster Net"

Використання роутерів дає змогу користувачеві призначати та змінювати маршрути проходження пакетів, оптимально розподілити мережевий трафік і обійти об'єкти, що перешкоджають обміну даними між об'єктами мережі.

Фізична реалізація мережі "Medium Cluster Net" представлена на рис. 22.

Під час побудови мережі слід враховувати, що в разі спільного використання різних трансиверів дистанція стійкого зв'язку S2 дорівнюватиме найменшому значенню S1,

де: S1 - дистанція для трансивера NRF24L01+PA+LNA (1 км);

S2 - дистанція для трансивера E01-2G4M27D (2 км).

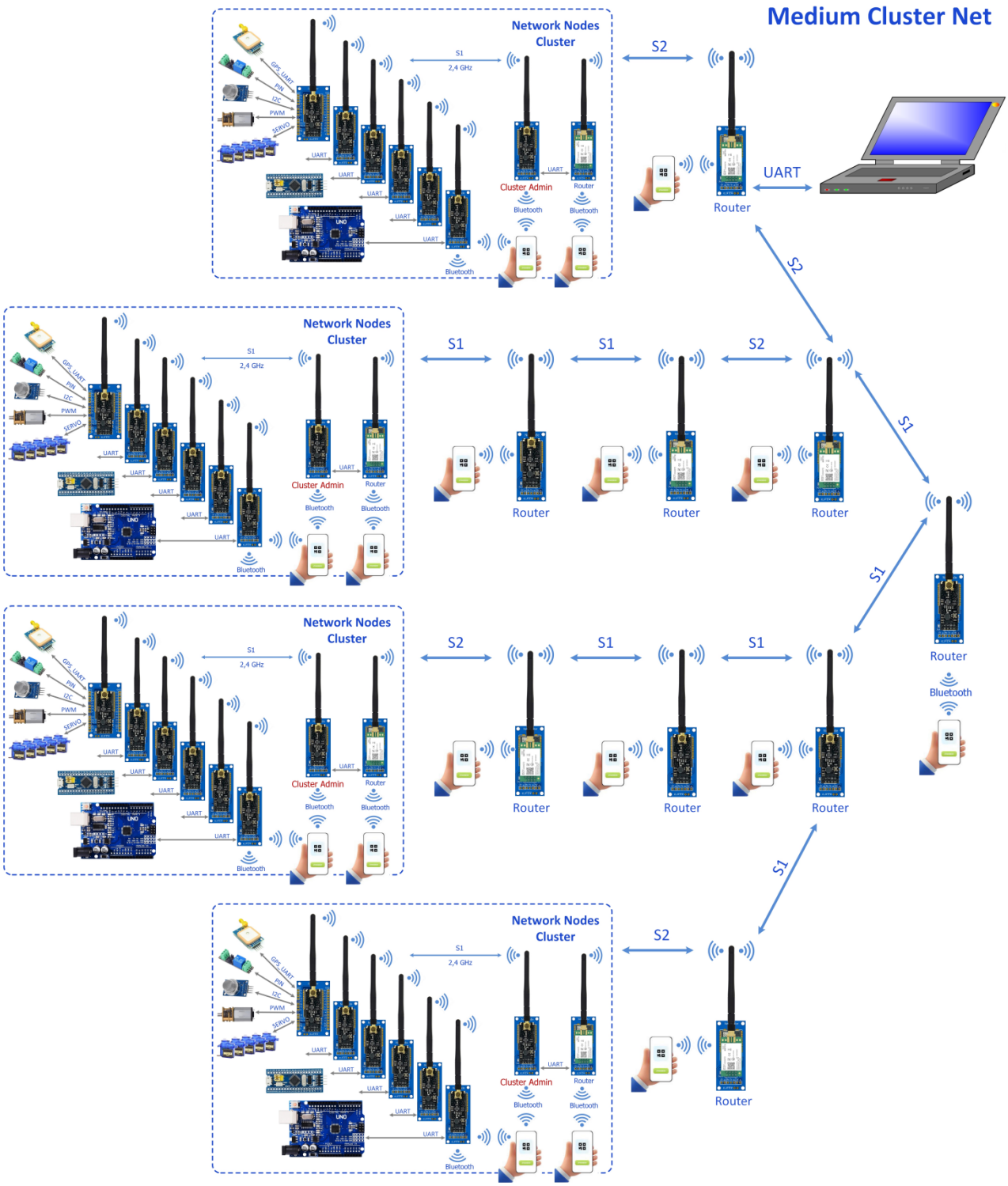


Рисунок 22 - Фізична реалізація мережі "Medium Cluster Net"

Модель "Union Cluster Net" об'єднує декілька локальних мереж різної архітектури в єдину систему. Використання мереж Internet та GSM дає можливість побудови глобальної мережі Easy Net Everywhere з урахуванням певних обмежень.

Архітектура мережі на основі моделі "Union Cluster Net" представлена на рис. 23.

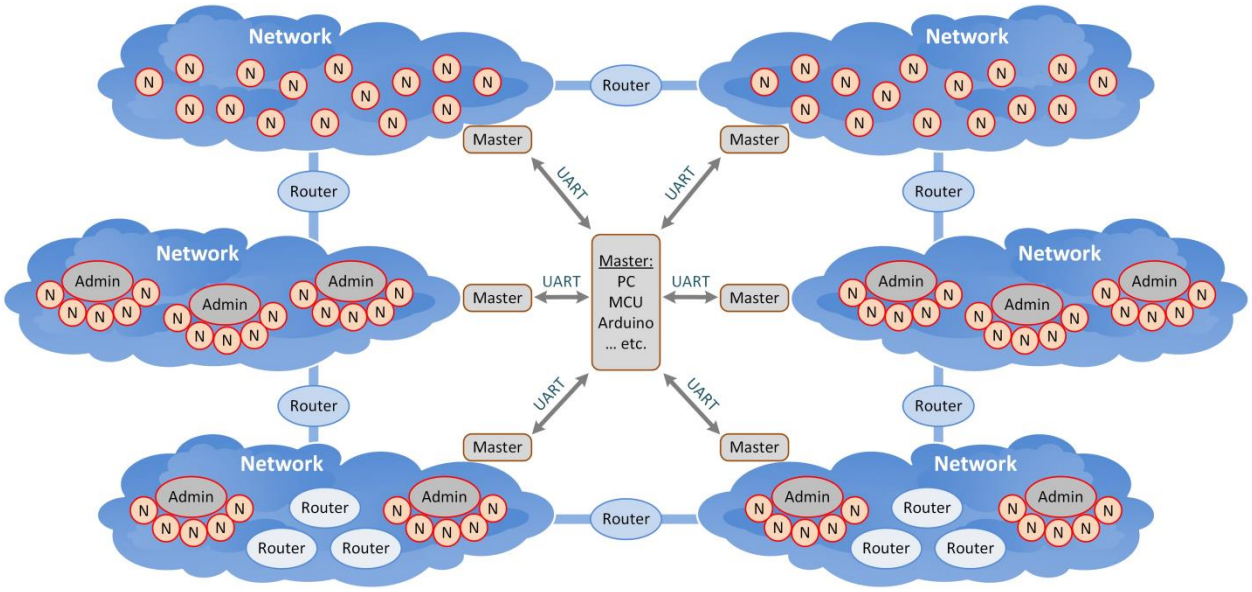


Рисунок 23 - Архітектура мережі на основі моделі "Union Cluster Net"

Адресація вузлів у мережі

Кожен вузол мережі має свою унікальну адресу. Повна адреса вузла складається з трьох компонентів: адреси мережі, адреси кластера і номера вузла в кластері.

Довжина адреси мережі становить 1 байт і адресує 254 мережі.

Довжина адреси кластера становить 4 біти і адресує 14 кластерів.

Довжина номера вузла становить 4 біти і адресує 15 вузлів.

Формат мережевої адреси наведено на рис. 24.

Рисунок 24 - Формат мережевої адреси

Поділ адресного простору мережі

Адресний простір мережі розділено на сегменти за функціональною ознакою пристроїв:

- вузли кластера мають номери: 1-15/0x01-0x0F;
- адміністратори кластера займають діапазон адрес: 0.0-13.0/0x00-0xD0;
- роутери та репітери займають діапазон адрес: R0-R30/0xE0-0xFE/.

Поділ адресного простору мережі на сегменти представлено на рис. 25.

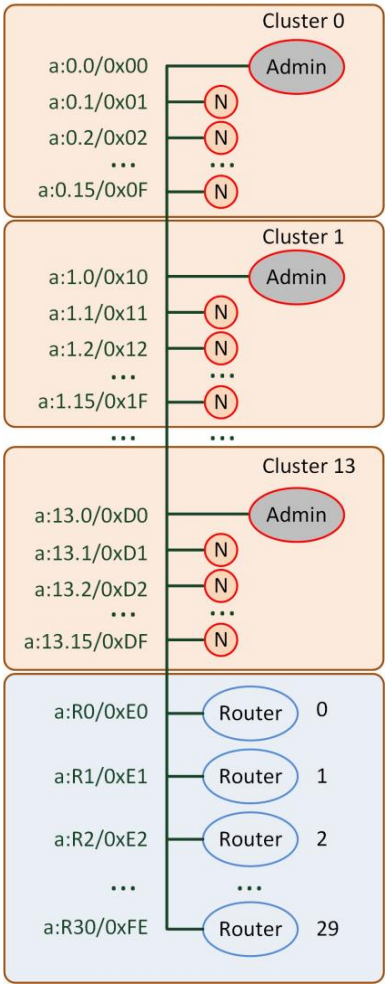


Рисунок 25 - Поділ адресного простору мережі на сегменти

Адреси вузлів мережі наведені в таблиці 1.

Таблиця 1 - Адреси вузлів мережі

Cluster Admin address		**Node address**		**Full Node address**		**Router address**			
alias:	hex:	alias:	hex:	alias:	hex:	alias:	hex:	alias:	hex:
0	0x00	1	0x01	0.1-1.15	0x01-0x0F	R0	0xE0	R16	0xF0
1	0x10	2	0x02	1.1-1.15	0x11-0x1F	R1	0xE1	R17	0xF1
2	0x20	3	0x03	2.1-2.15	0x21-0x2F	R2	0xE2	R18	0xF2
3	0x30	4	0x04	3.1-3.15	0x31-0x3F	R3	0xE3	R19	0xF3
4	0x40	5	0x05	4.1-4.15	0x41-0x4F	R4	0xE4	R20	0xF4
5	0x50	6	0x06	5.1-5.15	0x51-0x5F	R5	0xE5	R21	0xF5
6	0x60	7	0x07	6.1-6.15	0x61-0x6F	R6	0xE6	R22	0xF6
7	0x70	8	0x08	7.1-7.15	0x71-0x7F	R7	0xE7	R23	0xF7
8	0x80	9	0x09	8.1-8.15	0x81-0x8F	R8	0xE8	R24	0xF8
9	0x90	10	0x0A	9.1-9.15	0x91-0x9F	R9	0xE9	R25	0xF9
10	0xA0	11	0x0B	10.1-10.15	0xA1-0xAF	R10	0xEA	R26	0xFA
11	0xB0	12	0x0C	11.1-11.15	0xB1-0xBF	R11	0xEB	R27	0xFB
12	0xC0	13	0x0D	12.1-12.15	0xC1-0xCF	R12	0xEC	R28	0xFC
13	0xD0	14	0x0E	13.1-13.15	0xD1-0xDF	R13	0xED	R29	0xFD
Address range		15	0x0F	Address range		R14	0xEE	R30	0xFE
0.0-13.0	0x00-0xD0			0.1-13.15	0x01-0xDF	R15	0xEF		

Приклад адресації вузлів мережі

Якщо вузли належать до однієї мережі, то адреса мережі не вказується.

Приклад адресації вузлів мережі наведено на рис. 26.

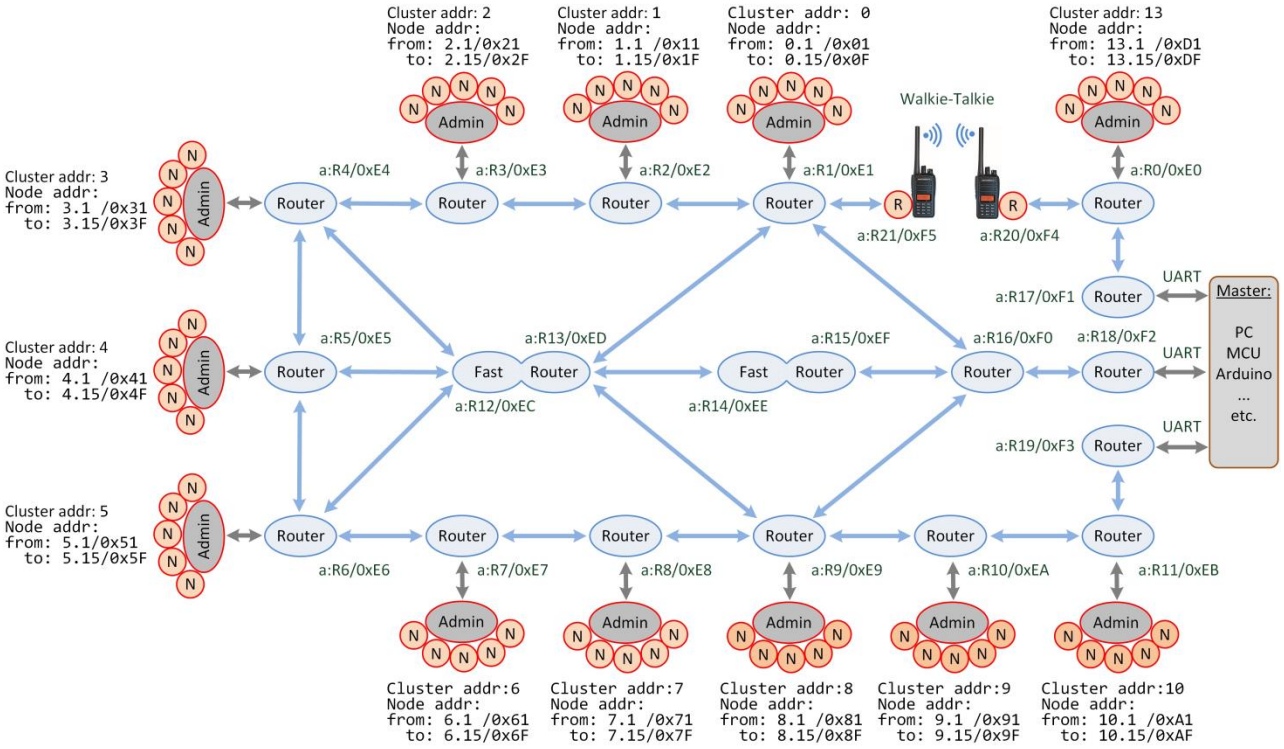


Рисунок 26 - Приклад адресації вузлів мережі

Призначення виводів друкованих плат вузлів мережі

Вузол "Controller" має виводи для керування зовнішніми пристроями та отримання сигналів від них (ADC, DAC, PWM, Servo, I/O), а також комунікаційні інтерфейси UART, I2C, SPI.

Призначення виводів вузла "Controller" представлено на рис.27.

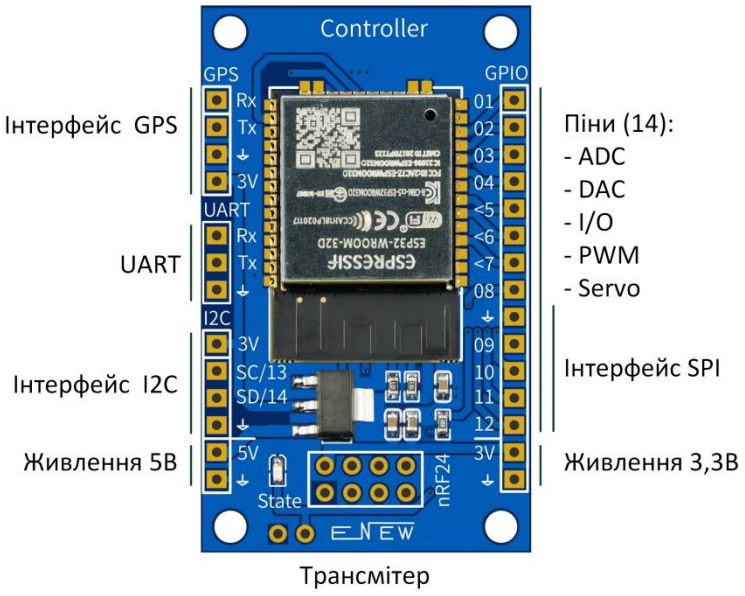


Рисунок 27 - Призначення виводів вузла "Controller"

Решта вузлів мережі мають у своєму складі тільки інтерфейси UART і Bluetooth (BLE).

Усі вузли живляться напругою 5 В і 3,3 В.

Вузли мережі: "Light Node", "Cluster Admin", "Net Router", "Net Master" і "Repeater" мають ідентичні друковані плати і призначення виводів. Відмінності є тільки в програмному забезпеченні та виконуваних функціях.

Призначення виводів перерахованих вище вузлів наведено на рис.28.

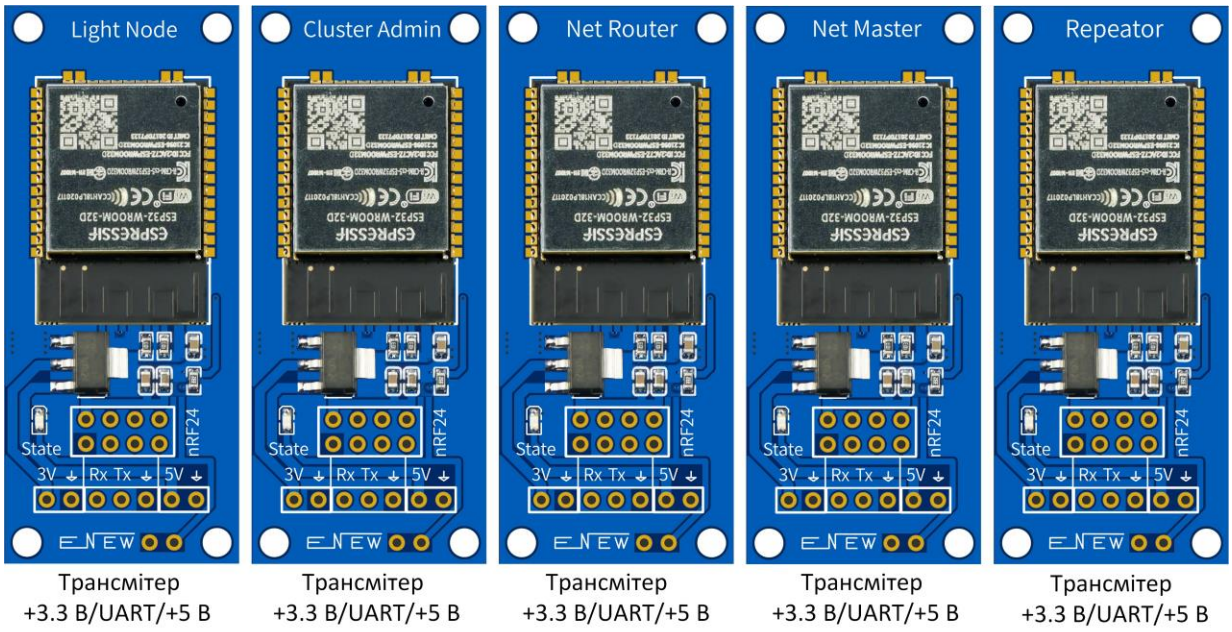


Рисунок 28 - Призначення виводів інших вузлів мережі

Підготовка вузлів мережі до роботи

Для підготовки вузла мережі до роботи необхідно під'єднати його до джерела живлення 5 В або 3,3 В, як зазначено на рисунках 27 і 28.

Для взаємодії користувача з вузлом через комп'ютер, через мікроконтролер або через плату Arduino, необхідно роз'єм UART вузла під'єднати до роз'єму UART відповідного пристрою і встановити швидкість 115200 baud.

Для підключення вузла до комп'ютера використовується будь-який конвертор UART-USB. До комп'ютера через USB-Hub можна підключити кілька вузлів мережі.

Після цього можна увімкнути живлення вузла і виконати відповідні налаштування вузла за допомогою будь-якої термінальної програми.

Налаштування вузла можна виконати через планшет/смартфон за допомогою програми "Serial Bluetooth Terminal" (автор Kai Morich).

Для цього достатньо з'єднатися з вузлом по інтерфейсу Bluetooth (BLE) і виконати відповідні налаштування.

Цю процедуру необхідно виконати для кожного вузла мережі.

Якщо всі підключення виконано правильно, то під час увімкнення живлення у вікні терміналу з'явиться таке повідомлення:

```
> Node 123 ready to start. Wait...
**********************
*  Easy Net EveryWhere
*  -------------------
*  Network.mode:   SIMPLE_NET
*  Radio.bitrate:  250Kb
*  UART.baud:      921600
*  Bluetooth:      ON
*  Bluetooth name: 111.123 NET_NODE
**********************
>> Controller 123 started
```

Це означає, що вузол працездатний і готовий до роботи. Після цього необхідно виконати налаштування параметрів вузла.

Для налаштування вузла необхідно скористатися АТ-командами, які можуть бути надіслані вузлу з вікна терміналу або з планшета/смартфона.

АТ-команди виконують функції інтерфейсу пристрою з користувачем, що дає змогу програмі керування пристроєм інкапсулювати виклики системних функцій.

Тестування мережі. Передача команд і даних

Адміністрування мережі, обмін інформацією в мережі та налаштування параметрів вузлів мережі здійснюється не тільки через порт UART комп'ютера/мікроконтролера, а й через планшет/смартфон за допомогою програми "Serial Bluetooth Terminal" (автор Kai Morich).

Для перевірки правильності роботи командних кнопок і працездатності вузлів мережі необхідно під'єднати вузли відповідно до рис. 29. На комп'ютері має бути встановлена будь-яка термінальна програма.

Тест якості зв'язку між двома вузлами запускається кнопкою "COUNT", яка передає вузлу АТ- команду *"AT+COUNTER target[,period]"*. Слід врахувати, що АТ-команда має обов'язковий параметр, який необхідно ввести, і необов'язковий. Його можна не вказувати.

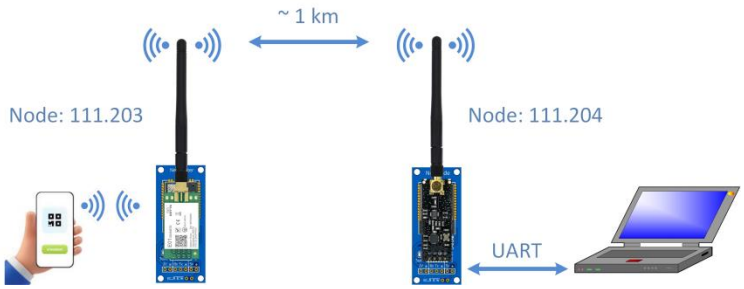
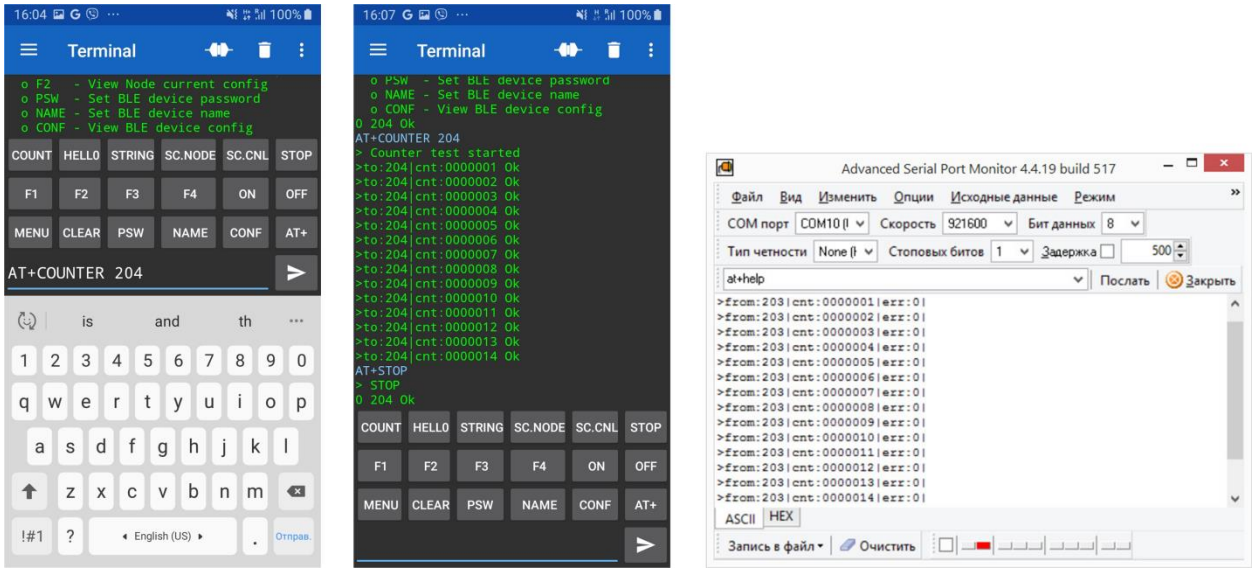


Рисунок 29 - Підключення вузлів мережі для тестування

Обов'язковим параметром є адреса вузла-одержувача, до якого буде звернення. Приклад введення показано на рис. 30.a.

Після правильного введення команди та натискання кнопки ">" запуститься тест інкрементного лічильника, значення якого передаватиметься вузлу-одержувачу. Процес виконання тесту відображатиметься у вікні терміналу на смартфоні, як показано на рис.30.b і у вікні терміналу на комп'ютері (рис.30.c).

Кількість помилок слугує критерієм для визначення якості зв'язку на обраному каналі.



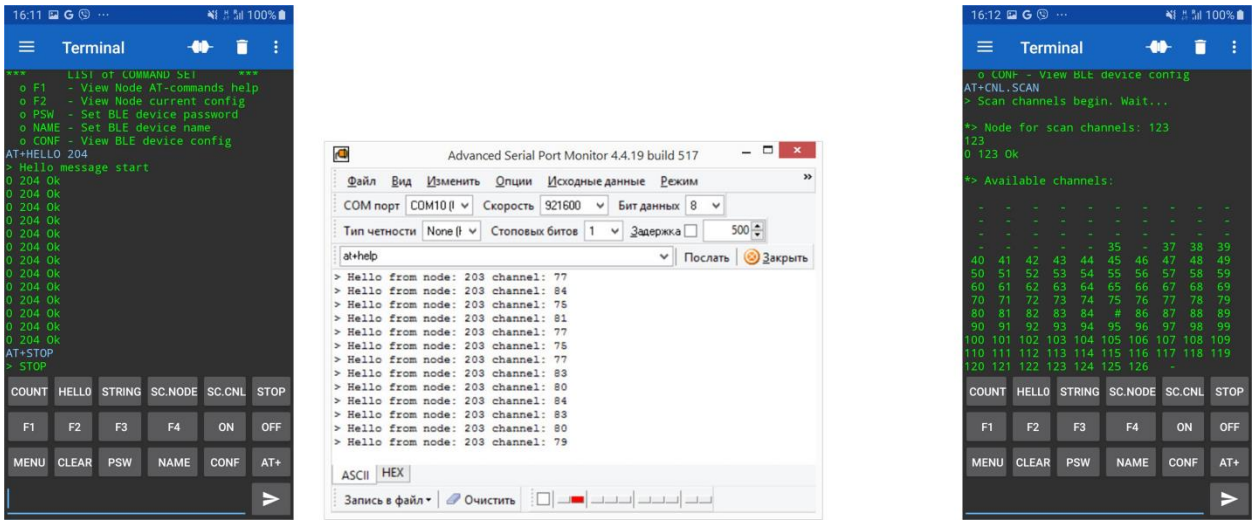
a) b) c)

Рисунок 30 - Запуск і виконання тестової команди "AT+COUNTER target[,period]"

Для тестування пропускної здатності каналу використовується тест *"HELLO"*. Тест запускається на кількох вузлах, які надсилають повідомлення "Hello from node" одному вузлу.

Після введення команди "AT+HELLO target[,period]" і натискання кнопки ">" запуститься тест. Процес виконання тесту відображатиметься у вікні терміналу на смартфоні, як показано на рис. 31.a і у вікні терміналу на комп'ютері (рис. 31.b). Кількість колізій, що виникають, слугує критерієм визначення пропускної здатності каналу.

На рис. 31.c відображено виведення у вікно термінала смартфона результату виконання команди сканування каналів "AT+CNL.scan". З результату сканування випливає, що зайнятими каналами є канали 0-34, а канали 37-126 можна використовувати. Символ " # " у списку каналів позначає головний канал мережі.



a) b) c)

Рисунок 31 - Виконання тестової команди "AT+HELLO target[,period]"

На рисунку 32 представлено виведення у вікно терміналу планшета повідомлень тестової команди "AT+HELLO target[,period]" у процесі виконання. У тесті беруть участь 6 вузлів.

Вузол 203 - одержувач, а вузли 204, 205, 206, 207, 208 - відправники.

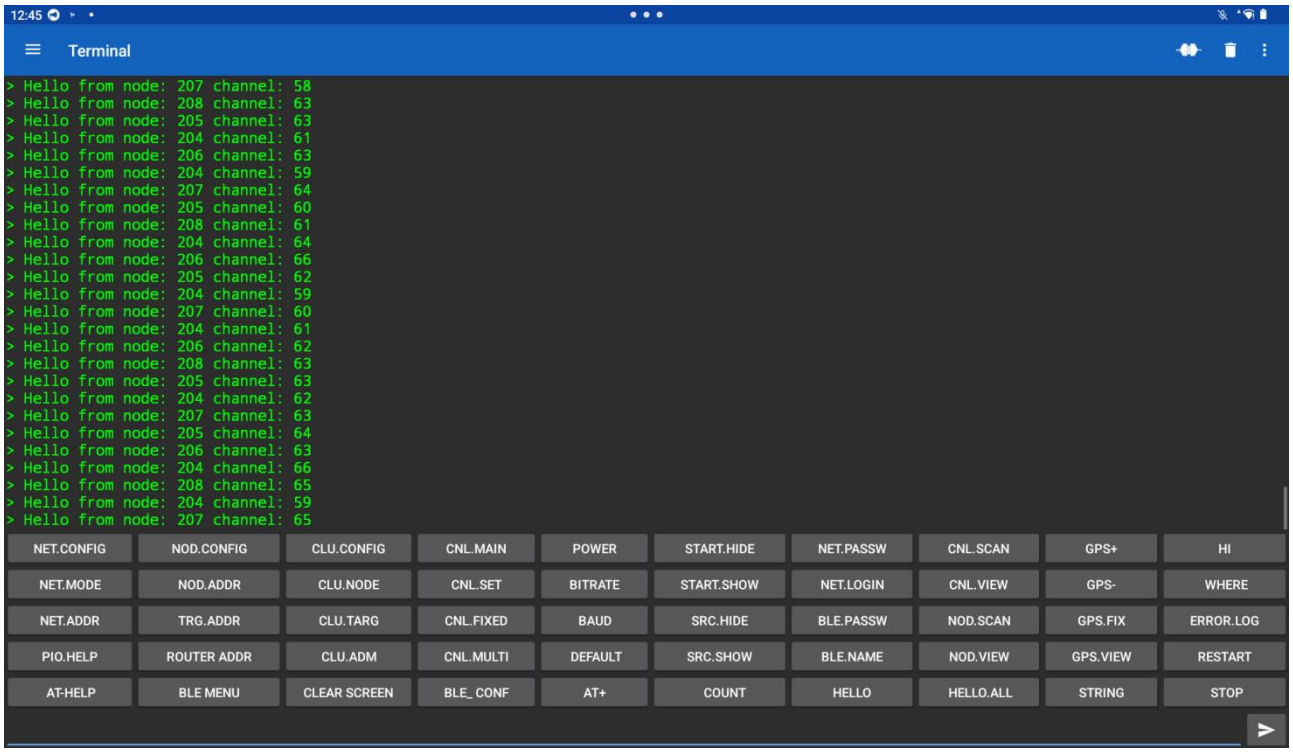


Рисунок 32 - Виконання тестової команди "AT+HELLO target[,period]" на 6 вузлах

На рисунку 33 представлено виведення повідомлень того самого тесту у вікна терміналів на комп'ютері через порти UART.

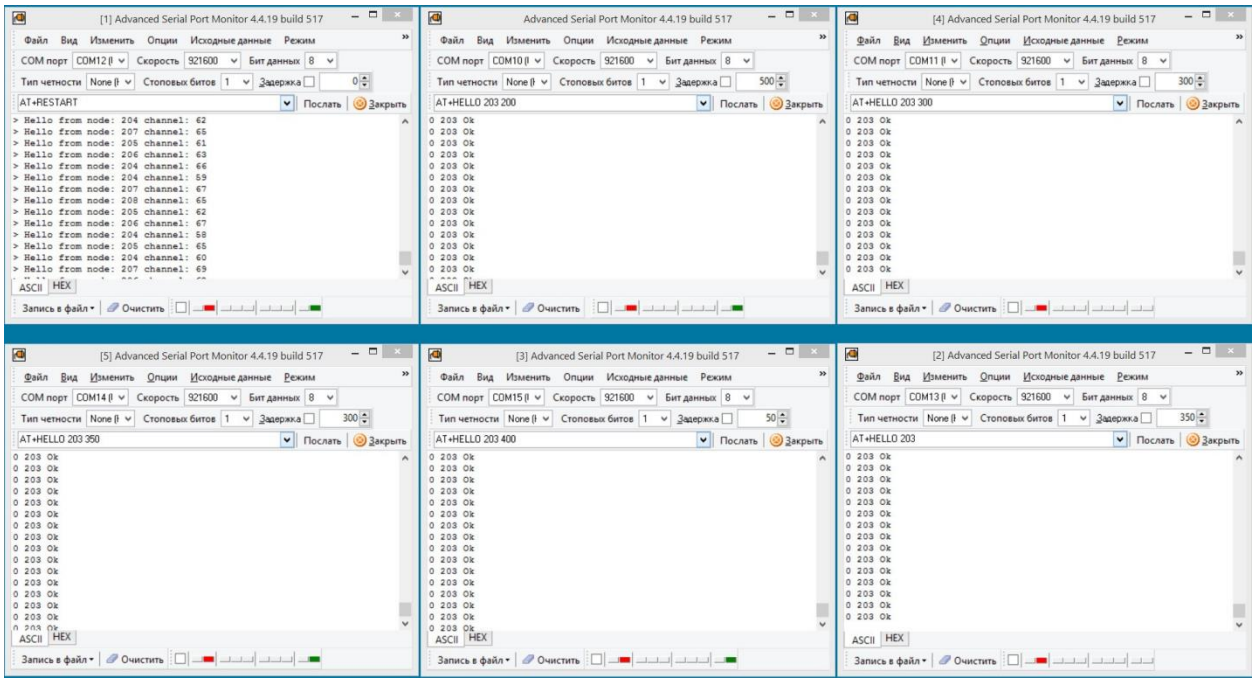


Рисунок 33 - Виконання тестової команди "AT+HELLO target[,period]" на 6 вузлах

Примітка:

Рядок "0 203 Ok" у вікні термінала (рис. 35) позначає:

0 - код квитанції успішної доставки пакета;

203 - адреса вузла-одержувача;

Ok - символьний еквівалент коду квитанції.

Перед початком роботи в мережі рекомендується встановити такі основні параметри:

Режим роботи мережі: команда *"AT+NET.mode m"*.

Для всіх режимів мережі встановити:

Адреса мережі: команда *"AT+NET.addr a"*.

Номер каналу мережі: команда *"AT+CNL.main n"*.

Швидкість порту UART: команда *"AT+BAUD bd"*.

Якщо обрано режим роботи мережі "Simple Net", то встановити:

Адреса вузла: команда *"AT+NOD.addr a"*.

Якщо обрано режим роботи мережі "Light Cluster Net", додатково встановити:

Номер адміна кластера: команда *"AT+CLU.adm n"*.

Номер вузла кластера: команда *"AT+CLU.node n"*.

Якщо обрано режим роботи мережі "Medium Cluster Net", додатково встановити:

Адреси роутерів: команда *"AT+ROUT.num n"*.

Адреси репітерів можна встановлювати в будь-якому режимі роботи мережі.

Подивитися поточні параметри вузла можна за допомогою команди: *"AT+NOD.config"*

Підключення обладнання для роботи в мережі

Підключення обладнання та організація процесу обміну даними в мережі є простим завданням. Усі пристрої підключаються до вузлів мережі через послідовний інтерфейс UART відповідно до рис. 34 и 35.

Комп'ютери та контролери можна підключати в будь-якій комбінації. Приклад під'єднання комп'ютерів до вузлів мережі наведено на рис. 34.

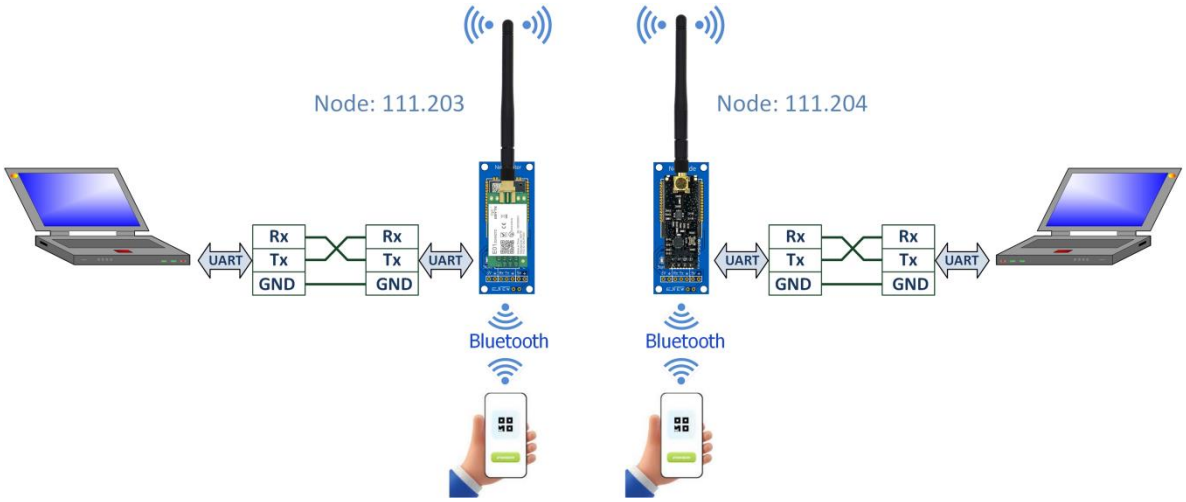


Рисунок 34 - Підключення комп'ютерів до вузлів мережі

Приклад підключення контролерів до вузлів мережі подано на рис. 35.

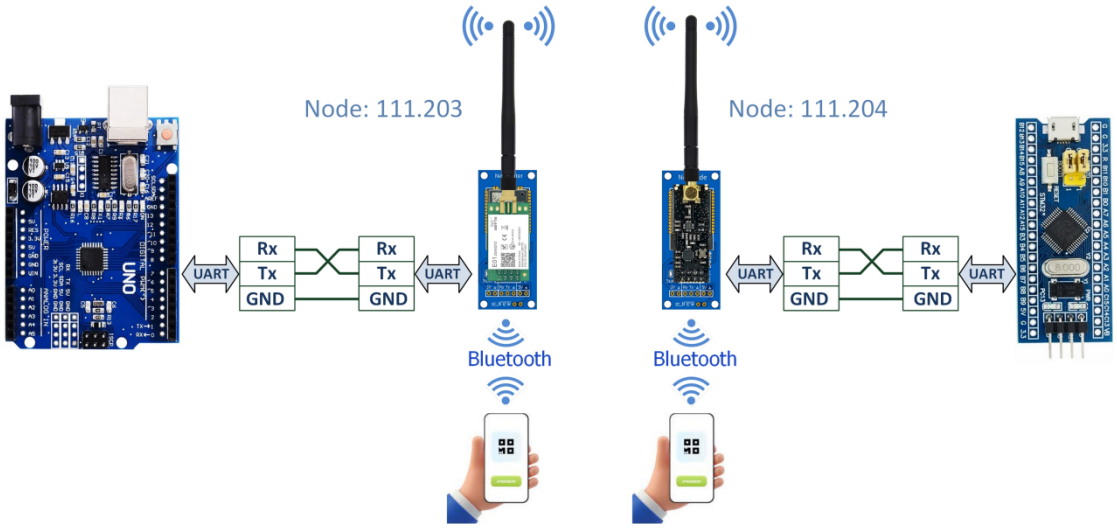


Рисунок 35 - Підключення контролерів до вузлів мережі

Якщо параметри вузлів мережі встановлено правильно, то мережа починає функціонувати. Перед початком експлуатації мережі рекомендується:

1. Просканувати канали та встановити номер головного каналу в середині найбільшої ділянки доступних каналів.

2. Виконати тестування за допомогою набору вбудованих тестів.

Обмін даними в мережі

Вузлу-одержувачу можуть бути надіслані будь-які дані у символьному та цифровому форматі.

Дані можуть бути форматовані, якщо дані є командним рядком зі списком параметрів або бути простим текстовим рядком.

Завдання парсингу даних лежить на користувачеві. Вузол-одержувач виводить у UART дані у тому порядку, як вони були відправлені вузлом-відправником.

Порядок проходження байтів у переданому повідомленні не змінюється. Вузол-одержувач приймає дані з мережі та виводить їх у порт UART у тому порядку, в якому вони надійшли в порт UART вузла-відправника.

Тобто для користувача процес передачі даних є прозорим, як показано на рис. 36.

Швидкість портів UART вузлів встановлюється користувачем з урахуванням особливостей приймальних та передавальних пристроїв.

Наприклад, швидкість порту UART вузла-відправника може бути 921600 baud, а швидкість порту UART вузла-приймача - 115200 baud.

Рисунок 36 – Порядок проходження байтів у повідомленні, що передається.

На рисунку 37 показаний приклад розміщення вузлів мережі на місцевості та можливі маршрути проходження даних.

Відстань між вузлами мережі при використанні штатної антени не повинна перевищувати 2 км. Якщо використовується антена Yagi з коефіцієнтом посилення 10 dBi або 25 dBi, то відстань між вузлами може бути збільшена до 5 і 20 км відповідно.

Слід враховувати, що лісосмуга є перешкодою для проходження радіохвиль діапазону 2.4 GHz, тому для обходу перешкоди необхідно використовувати додаткові роутери або репітери.

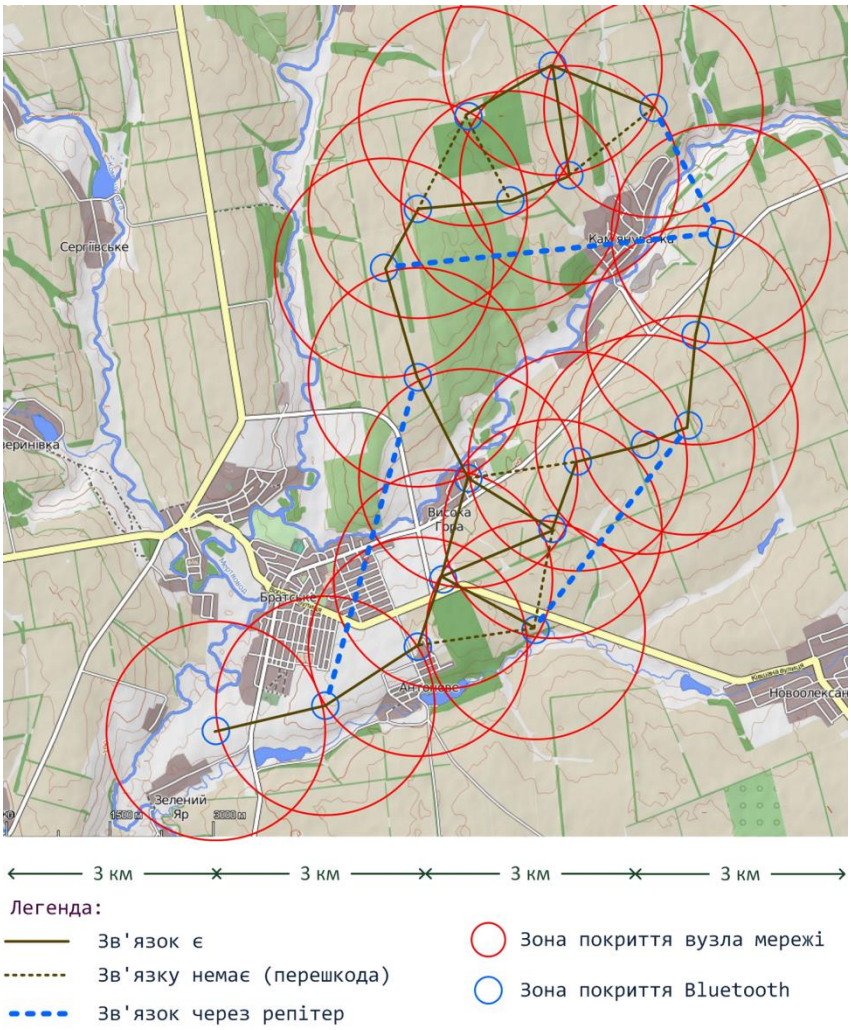


Рисунок 37 - Приклад розміщення вузлів мережі на місцевості

Приклад адресації вузлів і передачі даних

Перед надсиланням даних у мережі вузол-відправник має встановити адресу вузла одержувача в символьному або цифровому форматі. У цифровому форматі повідомлення більш компактне.

Встановлення адреси вузла-одержувача здійснюється трьома способами:

Спосіб 1: Використання AT-команди *AT+TRG.addr a.*

Адреса вузла-одержувача буде збережена в EEPROM. Усі наступні транзакції за замовчуванням здійснюватимуться тільки з цим вузлом.

Приклад:

```
AT+TRG.addr 203          //target address = 203
Hello! This is a simple message    //message to node 203
AT+CLU.targ 01.05   //target address:01.05(Cluster = 1 node = 5)
Hello! This is a simple message    //message to node 01.05
```

Спосіб 2: Встановлення адреси вузла-одержувача на початку повідомлення. Адреса в EEPROM не зберігається. Усі наступні транзакції будуть здійснюватися тільки з цим вузлом.

Приклад:

Символьний формат:

```
*203*Hello! This is a simple message        //message to node 203
*205*Hello! This is a simple message        //message to node 205
*01.05*Hello! This is a simple message      //message to node 01.05
*02.07*Hello! This is a simple message      //message to node 02.07
```

Цифровий формат:

```
#CB#Hello! This is a simple message    //message to node 203 = 0xCB
#CD#Hello! This is a simple message    //message to node 205 = 0xCD
#25#Hello! This is a simple message    //message to node 02.05
#27#Hello! This is a simple message    //message to node 02.07
```

Спосіб 3. Встановлення адреси вузла-одержувача в окремому повідомленні. Адреса в EEPROM не зберігається. Усі наступні транзакції здійснюватимуться тільки з цим вузлом.

Приклад:

Символьний формат:

```
*203*                              //target address = 203
Hello! This is a simple message        //message to node 203
*02.07*
Hello! This is a simple message        //message to node 02.07
```

Цифровий формат:

```
#CB#                               //target address = 203/0xCB
Hello! This is a simple message        //message to node 203
#25#
Hello! This is a simple message        //message to node 02.05
```

Надсилання даних вузлу-одержувачу

Вузлу-одержувачу можуть бути надіслані будь-які дані в символьному та цифровому форматі.

Приклад 1:

Передання вузлу 203 команди !XXXX! з параметрами в символьному форматі.

```
String DATA_OUT = "*203*!XXXX!12,12345,234567,345.678";
UART.write(DATA_OUT);    //send data to network
```

Передача вузлу 01.05 команди !XXXX! із параметрами у символьному форматі:

```
String DATA_OUT = "*01.05*!XXXX!12,12345,234567,345.678";
UART.write(DATA_OUT);    //send data to network
```

На стороні вузла-одержувача дані можна прийняти в такий спосіб:

```
#include “Parser.h”
enum   package{_cmd,_parm_1,_parm_2,parm_3,_parm_4};    //data format
byte DATA_IN[150];
String cmd;
byte var_8; short var_16;
int32 var_32;float var_fl;
//
//== parsing
parse_data(DATA_IN);
//== get parameters
cmd = get_token_string(_cmd);           // cmd = !XXXX!
var_8 = get_token_byte(_parm_1);        // var_8 = 12
var_16 = get_token_short(_parm_2);      // var_16 = 12345
var_32 = get_token_int32(_parm_3);      // var_32 = 234567
var_fl = get_token_float(_parm_4);      // var_fl = 345.678
```

Приклад 2:

Передача вузлу 203 команди !XXXX! у цифровому форматі з параметрами без роздільників:

```
enum package{cmd = 3,data}; //data format
char DATA_OUT[15];
//
DATA_OUT[0] = '#';       //address tag
DATA_OUT[1] = 0xCB;      //target address = 203
```

```
    DATA_OUT[2] = '#';        //address tag
    DATA_OUT[cmd] = 0x25;      //hex view of command !XXXX! (for
example)
    //== put data to array
    for(int8 i = data;i<10;i++){
       DATA_OUT[i] = i;
    }
    UART.write(DATA_OUT);         //send data to network
```

Висновки

Практична реалізація бездротової локальної мережі для застосування в територіально-розподілених системах, які потребують наявності бездротового зв'язку з об'єктами управління з гарантованою доставкою команд і даних зі швидкістю 250 Kbps у радіусі до 10 км є результатом проведених дослідницьких, проектних і конструкторських робіт у рамках науково-дослідної теми «Створення мобільної мережі 2.4 GHz з адаптивною аморфною топологією для управління роєм БПЛА і робототехнічних об'єктів», реєстраційний № 0120U104088.

Архітектуру бездротової локальної мережі покладено в основу системи бездротового керування робототехнічними пристроями, дронами та іншими об'єктами, а також в основу платформи для розроблення та реалізації проєктів "Internet Of Things", систем класу "Smart Home" і подібних малих систем.

Топологія бездротової мережі не детермінована, аморфна і змінюється під час переміщення об'єктів мережі в просторі. При цьому втрачаються одні зв'язки і виникають інші. Таблиці маршрутизації постійно оновлюються.

Поточна версія реалізації мережі забезпечує:

- стабільну взаємодію вузлів мережі при зміні топології мережі;
- обмін даними між вузлами мережі як безпосередньо між собою, так і через ретранслятори та шлюзи без втрат інформаційних пакетів;
- масштабування мережі із заданою топологією з охопленням площі від 0.04 км2 (мінімальна потужність, відсутність ретрансляції пакетів, відсутність перешкод на місцевості) до 65 км2 (максимальна потужність, 3 ретранслятори в ланцюжку, є перешкоди на місцевості);
- низький рівень випромінювання в діапазоні 2.4 GHz що є необхідною умовою для підвищення порога виявлення роботи вузлів у мережі.

Таким чином, досягнуті результати повною мірою відповідають розрахунковим і є основою для подальшого вдосконалення мережі та підвищення її експлуатаційних характеристик.

References:

IEEE 802.15.4-2020 - IEEE Standard for Low-Rate Wireless Networks. Standards Committee : C/LM - LAN/MAN Standards Committee. 2020.05.06. URL: https://standards.ieee.org/standard/802_15_4-2020.html (дата звернення: 12.03.2023).

Recommendation G.9959. URL: https://www.itu.int/rec/T-REC-G.9959-201310-S!Amd1/en (дата звернення: 12.03.2023).

LoRaWAN™ Specification, N.Sornin (Semtech), M.Luis (Semtech), T.Eirich (IBM), T.Kramp (IBM), O.Hersent (Actility), V1.0, 2015 January.

Смирнов В.В., Смирнова Н.В. Архитектура контроллера узла адаптивной мобильной сети с аморфной топологией / Збірник наукових праць «Центральноукраїнський науковий вісник. Технічні науки» - (3)-34 - Кропивницький: ЦНТУ, 2020. – С. 12-21. (Фахове видання)
DOI: https://doi.org/10.32515/2664-262X.2020.3(34).12-21.

Смирнов В.В., Смирнова Н.В.Архітектура адаптивної бездротової локальної мережі для управління об'єктами і пристроями. Загальнодержавний міжвідомчий науково-технічний збірник. Конструювання, виробництво та експлуатація сільськогосподарських машин. Кропивницький: ЦНТУ, 2020. Вип. 50. С. 219-229 (Фахове видання). http://zbirniksgm.kntu.kr.ua/pdf/50/28.pdf. DOI: https://doi.org/10.32515/2414-3820.2020.50.219-229.

Смирнов В.В., Смирнова Н.В. Бездротова локальна мережа класу Smart Home на базі модулів сплітерів-репітерів. Загальнодержавний міжвідомчий науково-технічний збірник Конструювання, виробництво та експлуатація сільськогосподарських машин. Кропивницький: ЦНТУ, 2021. Вип. 51. С. 195-202 (Фахове видання). http://zbirniksgm.kntu.kr.ua/pdf/51/%E2%84%9651_2021.pdf. DOI: https://doi.org/10.32515/2414-3820.2021.51.195-202.

Смірнов В.В., Смірнова Н.В. Мобільна mesh-мережа для управління роєм об'єктів. Центральноукраїнський науковий вісник. Технічні науки. 2023. Вип. 7(38), ч.II. С. 3-11 (Фахове видання). DOI: https://doi.org/10.32515/2664-262X.2023.7(38).2.3-11.

CONTENTS

Norwegian University of Life Sciences

INTERNATIONAL SECURITY STUDIOS: managerial, technical, legal, environmental, informative and psychological aspects

international collective monograph

Volume I

M 58 International security studios: managerial, technical, legal, environmental, informative and psychological aspects. *International collective monograph. Volume I. NMBU, Research and Education*. 2024. – 700 p.

The International collective monograph is the result of the generalization of the conceptual work of scientists who consider current topics from such fields of knowledge as: management, technical sciences, law, ecology, information sciences and psychological sciences through the prism of international security studies.

For scientists, educational staff, PhD candidates, masters of educational institutions, university faculties, stakeholders, managers and employees of management bodies at various hierarchical levels, and for everyone, who is interested in current problems of management, technical sciences, law, ecology, information sciences and psychological sciences through the prism of international security studies.

ISBN 978-82-327-0549-9