

INSTITUTE OF PUBLIC ADMINISTRATION AFFAIRS

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

International collective monograph.

Volume II.

Lublin, Polska 2025

UDC 327(100)-049.5

I 61

DOI 10.5281/zenodo.10.....

Recommended for publication by the by INSTITUTE OF PUBLIC ADMINISTRATION AFFAIRS

№ 4 dated 2025-04-15

Editorial committee:

JANUSZ NICZYPORUK, Doctor of Legal Sciences, Professor, Professor Maria Curie Skłodowska University (Lublin, Poland);

OLHA BALYNSKA, Doctor of Law, Professor, Lviv State University of Internal Affairs (Lviv, Ukraine);

OLEG BATIUK, Doctor of Law, Associate Professor, Chairman of the Board of the NGO "IESF" (Kyiv, Ukraine);

MAKSYM KORNIENKO, Doctor of Law, Professor, Vice-rector of Odessa State University of Internal Affairs (Odessa, Ukraine).

Reviewers:

SERHII BIELAI, Doctor of Sciences in Public Administration, Professor, Professor of the State Security Department National Academy of the National Guard of Ukraine (Kharkiv, Ukraine);

SVITLANA CHERNETA Doctor of Pedagogical Sciences, Professor, Lesya Ukrainka Volyn National University, (Luts'k, Ukraine).

VALERIY KOLESNYK, Doctor of Legal Sciences, Professor, Professor National Academy of Security Service of Ukraine (Kyiv, Ukraine).

Authors: N. Andrushkevych; A. Avsiievych; O. Batiuk; L. Danylivskyi; A. Pasichnyk; V. Beschastnyy; Yu. Bilash; V. Borysov; O. Grechanyk; S. Dementiev; S. Merinova; N. Diachenko; S. Fimyar; V. Glukhova; O. Haitan; L. Ibrahimova; S. Nykyporets; Y. Kotko; I. Kovtaniuk; S. Nykyporets; H. Kukharchuk; A. Terletskii.

M 58 International security studios: managerial, technical, legal, environmental, informative and psychological aspects. International collective monograph. Volume II. ISAP, Research and Education. 2025. – 436 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 978-83-8011-444-7

© ISAP 2025;

© The collective of authors 2025



Creative Commons Attribution 4.0 International

AUTHORS:

CHAPTER 1.

Nataliia ANDRUSHKEVYCH

PhD in Economics, Associate Professor of the Department of Management and Social and Humanitarian Disciplines, Cherkasy branch of Private Higher Educational Establishment «European University», (Cherkasy city, Smilianska st., 83)

natalia.andrushkevich@e-u.edu.ua
<https://orcid.org/0009-0006-2154-4068>

CHAPTER 3.

Oleg BATIUK

Doctor of Legal sciences, Assistant Professor, Professor of the Department of National Security, Lesya Ukrainka Volyn National University (Luts'k, Ukraine)

olegbatiukibrlpnt@gmail.com
<https://orcid.org/0000-0002-2291-4247>

Loenid DANYLIVSKYI

Senior Lecturer of the Department of Intelligence at the Kyiv Institute of the National Guard of Ukraine, Major General (Retired),

l.danilevskiy@kr.net
<https://orcid.org/0000-0003-1995-7980>

Andriy PASICHNYK

Lecturer at the Department of Military Communications and Informatization, National Academy of National Guard of Ukraine

pasechnik81@gmail.com
<https://orcid.org/0000-0001-9570-9888>

CHAPTER 5.

Yuliana BILASH

Candidate of Science/Hons. Science, Associate Professor of the Department of Labor Protection and Technological Equipment in Animal Husbandry, Lviv National University of Veterinary Medicine and Biotechnology named after S.Z. Gzhytsky (Pekarska, 50, Lviv, Ukraine)

ulianabilach@gmail.com
<https://orcid.org/0000-0002-8890-667X>

CHAPTER 2.

Alla AVSHEVYCH

PhD student, specialty D8 Law, Ph.D. Candidate Educational and Scientific Institute of Law named after Volodymyr the Great, Private Joint-Stock Company «Interregional Academy of Personnel Management»

taisha1878@gmail.com
<https://orcid.org/0000-0002-8192-8569>

CHAPTER 4.

Victor BESCHASTNYI

Head of Secretariat of the Constitutional Court of Ukraine, Doctor of Science of Law, Full Professor, Honored Lawyer of Ukraine,

beschastnyy.vm@gmail.com
<https://orcid.org/0000-0002-4650-7371>

CHAPTER 6.

Volodymyr BORYSOV

Candidate of Philology, Associate Professor, Vice-Rector for Educational & Scientific Work, H. S. Skovoroda Kharkiv National Pedagogical University (Kharkiv, Ukraine)

prorektor_borysov@hnpu.edu.ua
<https://orcid.org/0000-0001-7468-727X>

Olena GRECHANYK

Candidate of Pedagogical Sciences, Associate Professor, Head of the Department of Management and Economics, H. S. Skovoroda Kharkiv National Pedagogical University (Kharkiv, Ukraine)

grechaniklena@ukr.net
<https://orcid.org/0000-0002-4671-0724>

AUTHORS:

CHAPTER 7.

Serhii DEMENTIEV

candidate of Technical Sciences (Ph. D.), Associate Professor at Vinnytsia Trade and Economic Institute, Department of Information Systems and Technologies, (25, Khmelnytske shose, Vinnytsia, 21050, Ukraine)

s.dementiev@vtei.edu.ua

<https://orcid.org/0009-0006-1322-6756>

Svitlana MERINOVA

candidate of Economic Sciences (Ph. D.), Associate Professor at Vinnytsia Trade and Economic Institute, Department of Information Systems and Technologies, (25, Khmelnytske shose, Vinnytsia, 21050, Ukraine)

s.merinova@vtei.edu.ua

<https://orcid.org/0000-0001-6563-5320>

CHAPTER 9.

Svitlana FIMYAR

Candidate of Economics, Associate Professor of the Department of Economics, Finance, Accounting, Mathematical and Information Disciplines Cherkasy Branch of the Ukrainian Higher Education Establishment European University (83, Smilyanska str., Cherkasy, 18008, Ukraine)

fimyar@ukr.net

<https://orcid.org/0000-0003-0432-2587>

CHAPTER 11.

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 8.

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 Odesa Law Academy National University (210, Kharkiv highway, Kyiv, 02121, Ukraine)

n.diachenko@ukr.net

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

CHAPTER 10.

Valentyna GLUKHOVA

PhD in Economics, Associate professor Associate professor of the Department of Accounting and Finance, Kremenchuk Mykhailo Ostrohradskyi National University, (20, University Street, Kremenchuk, 39600, Ukraine)

Glukhova710@gmail.com

<https://orcid.org/0000-0003-3120-9651>

CHAPTER 12.

Liudmyla IBRAHIMOVA

senior English language lecturer? Vinnytsia National Technical University, Department of Foreign Languages, (95, Khmelnytske shose, Vinnytsia, 21021, Ukraine)

milatulchak@gmail.com

<https://orcid.org/0000-0002-9265-2449>

Svitlana NYKYPORETS

senior English language lecturer? Vinnytsia National Technical University, Department of Foreign Languages, (95, Khmelnytske shose, Vinnytsia, 21021, Ukraine)

fotinia606@gmail.com

<https://orcid.org/0000-0002-3546-1734>

AUTHORS:

CHAPTER 13.

Yana KOTKO

PhD in Economics, Associate Professor of the
Department of Economics and Business,
State Biotechnological University,
(Kharkiv, Ukraine, Alchevskikh str. 44)

kotkoyana@ukr.net

<https://orcid.org/0000-0001-6611-8130>

CHAPTER 14.

Inna KOVTANIUK

Teacher at the Department of Informatics and
Information and Communication Technologies,
Tychyna Uman State Pedagogical University
(2, Sadova str, Uman, 20300, Ukraine)

i.kryvoruchko@udpu.edu.ua

<https://orcid.org/0000-0002-9886-9315>

CHAPTER 15.

Svitlana NYKYPURETS

senior English language lecturer
Vinnytsia National Technical University,
Department of Foreign Languages,
(95, Khmelnytske shose, Vinnytsia, 21021,
Ukraine)

fotinia606@gmail.com

<https://orcid.org/0000-0002-3546-1734>

CHAPTER 16.

Anatoliy TERLETSKII

Doctor of philosophy, Lecturer of the Department
of State and Legal Disciplines
Odessa State University of Internal Affairs

anatoliyterletskii@gmail.com

<https://orcid.org/0009-0000-4767-9768>

Halyna KUKHARCHUK

English language lecturer,
Vinnytsia National Technical University,
Department of Foreign Languages,
(95, Khmelnytske shose, Vinnytsia, 21021,
Ukraine)

galinakup07@gmail.com

<https://orcid.org/0009-0003-7877-1921>

CHAPTER 1. FORMATION OF A MECHANISM FOR STRATEGIC PLANNING AND MANAGEMENT OF SUSTAINABLE DEVELOPMENT OF AN INDUSTRIAL ENTERPRISE

Nataliia ANDRUSHKEVYCH

PhD in Economics, Associate Professor

of the Department of Management and Social and Humanitarian Disciplines,
Cherkasy branch of Private Higher Educational Establishment «European University»,
(Cherkasy city, Smilianska st., 83)

natalia.andrushkevich@e-u.edu.ua

<https://orcid.org/0009-0006-2154-4068>

Abstract. The system of management of sustainable development of an enterprise, taking into account the dynamism of the management object, the strict focus of the system on a certain result, and as a result of its being under the constant influence of frequently changing factors, has formed into a capacious, multifaceted set of elements, the "quality" of each of which determines the development of a particular enterprise. Despite the presence of deeply studied and repeatedly applied methods, models, management strategies, the presence of a large number of means and methods of analyzing economic sustainability, the methodology for identifying factors affecting the sustainable development of an enterprise, the system is unique for each business entity. Also, the management of sustainable development of an enterprise must be carried out taking into account certain principles. The analysis of the principles of sustainable development management allowed us to identify two groups of principles: general (classical) management principles and specific (inherent specifically in sustainable development).

An author's set of principles of sustainable development management of an enterprise is proposed, including general principles (target orientation, systematicity, complexity, scientific validity, modeling, relevance, multivariance, comparability and measurability, digitality, innovation); the latter two as principles of sustainable development management of an enterprise are stated for the first time, and specific (characterizing environmental, social and economic development). The specification of the implementation of the principles of sustainable development management of an enterprise is considered, which provides for a review of possible measures and types of activities for the implementation of the process of sustainable development management of an enterprise.

These circumstances reveal the main and most difficult task facing management entities with decision-making functions, which is to create an individual strategy for its development for the enterprise by applying a management mechanism based on the characteristics of the organization.

The stages of the sustainable development management mechanism of industrial enterprises are considered, as well as the factors that influence the studied mechanism. The elements that are part of the sustainable development management mechanism are determined - economic and organizational, management elements and business philosophy. The author's algorithm for assessing the effectiveness of the sustainable development management mechanism is proposed, recommendations for improving this mechanism are developed.

The sustainable development management mechanism of industrial enterprises is proposed,

which is based on the principles of a systems approach, which provide for the implementation of interrelated processes of identifying and assessing risk factors of activity, as well as making appropriate management decisions with subsequent control of their results in order to promptly minimize the negative impact of risk factors on the economic, environmental and social spheres.

Keywords: management systems, industrial enterprises, enterprise management, sustainable development of the enterprise, principles of development management, sustainable development management mechanism.

ФОРМУВАННЯ МЕХАНІЗМУ СТРАТЕГІЧНОГО ПЛАНУВАННЯ ТА УПРАВЛІННЯ СТАЛИМ РОЗВИТКОМ ПРОМИСЛОВОГО ПІДПРИЄМСТВА

Анотація. Система управління сталим розвитком підприємства зважаючи на динамічність об'єкта управління, суворой спрямованості системи на певний результат, а як внаслідок її знаходження під постійним впливом факторів, що часто змінюються, сформувалася в ємну, багатогранну сукупність елементів, від «якості» кожного з яких залежить розвиток окремо взятого підприємства. Незважаючи на наявність глибоко вивчених і неодноразово застосовуваних методів, моделей, стратегій управління, наявності великої кількості засобів і способів аналізу господарської стійкості, методології виявлення факторів, що впливають на сталий розвиток підприємства, система для кожного суб'єкта господарської діяльності унікальна. Також, управління сталим розвитком підприємства має здійснюватися з урахуванням певних принципів. Проведений аналіз принципів управління сталим розвитком дозволив виявити дві групи принципів: загальні (класичні) принципи управління та специфічні (притаманні саме сталому розвитку).

Запропоновано авторський набір принципів управління сталим розвитком підприємства, включає загальні принципи (цільова орієнтація, системність, комплексність, наукова обґрунтованість, модельність, релевантність, багатоваріантність, порівнянність і вимірність, цифровість, інноваційність); останні два як принципи управління сталим розвитком підприємства заявлені вперше, та специфічні (характеризуючі екологічний, соціальний та економічний розвиток). Розглянуто конкретизацію реалізації принципів управління сталим розвитком підприємства, що передбачає огляд можливих заходів та видів діяльності з реалізації процесу управління сталим розвитком підприємства.

Зазначені обставини виявляють основне і найскладніше завдання, що стоїть перед суб'єктами управління, що мають функції прийняття рішень, що полягає у створенні індивідуальної для підприємства стратегії його розвитку за допомогою застосування механізму управління виходячи з особливостей організації.

Розглядаються етапи механізму управління сталим розвитком промислових підприємств, і навіть чинники, які впливають на досліджуваний механізм. Визначено елементи, що входять до складу механізму управління сталим розвитком – економічно-організаційні, елементи управління та філософії ведення бізнесу. Запропоновано авторський алгоритм оцінки ефективності механізму управління сталим розвитком, розроблено рекомендації щодо вдосконалення даного механізму.

Запропоновано механізм управління сталим розвитком промислових підприємств, який заснований на принципах системного підходу, що передбачають реалізацію взаємопов'язаних процесів виявлення та оцінки ризикових факторів діяльності, а також прийняття відповідних управлінських рішень з подальшим контролем їх результатів з метою своєчасної мінімізації негативного впливу ризикових факторів на економічну, екологічну та соціальну сфери.

Ключові слова: системи управління, промислові підприємства, управління підприємством, сталий розвиток підприємства, принципи управління розвитком, механізм управління сталим розвитком.

Вступ. На сучасному етапі розвитку світової економіки, який характеризується глибокою інтеграцією виробничих відносин у глобальну ринкову систему, відбувається подальше ускладнення організаційних структур підприємств. Це проявляється у розширенні їхньої просторової протяжності, збільшенні кількості виконуваних функцій, зростанні рівня взаємозалежності між підрозділами, а також ускладненні процесів прийняття управлінських рішень. У таких умовах постає необхідність у комплексному врахуванні широкого спектра факторів зовнішнього та внутрішнього середовищ при організаційному проектуванні та стратегічному управлінні підприємством.

З огляду на зазначене, промислове підприємство слід розглядати як складну організаційну систему, що функціонує в умовах високої турбулентності та динамічних змін ринкового середовища. Зокрема, сучасні виклики, пов'язані з технологічним прогресом, інноваційними трансформаціями, нестабільністю економічного та політичного середовища, екологічними обмеженнями та змінами споживчих пріоритетів, зумовлюють зростаючу потребу у впровадженні ефективних механізмів управління підприємствами. У зв'язку з цим особливої актуальності набуває питання забезпечення сталого функціонування та розвитку промислових суб'єктів господарювання, що вимагає формування дієвої системи стратегічного планування.

Сталий розвиток підприємств у сучасних умовах неможливий без глибокого аналізу поточного стану, визначення довгострокових цілей та побудови стратегії їх досягнення. При цьому критично важливою є спроможність управлінського персоналу не лише орієнтуватися в сучасних методах управління, але й оперативно адаптувати їх до специфічних умов діяльності підприємства. У цьому контексті зростає значення системного підходу до стратегічного планування, що передбачає синергетичне поєднання економічних, соціальних та екологічних чинників розвитку.

Для досягнення сталого зростання та ефективної інтеграції національної промисловості у світову економіку необхідні комплексні зусилля з боку підприємств, державних інституцій та наукової спільноти. Зокрема, це включає розробку та впровадження сучасних управлінських концепцій, що відповідають реаліям ринку, а також удосконалення механізмів стратегічного планування.

Ефективне стратегічне планування передбачає розробку системи обґрунтованих управлінських рішень, що визначають послідовність розвитку підприємства, використання методів аналізу ризиків, прогнозування та адаптивного управління. У цьому контексті особливого значення набуває створення механізму стратегічного управління сталим розвитком підприємств, який би враховував особливості їхньої діяльності, динаміку змін у зовнішньому середовищі та забезпечував формування ефективних стратегічних напрямів розвитку.

Зважаючи на зростаючу нестабільність та мінливість економічного середовища, підприємствам необхідно мати комплексний управлінський механізм, що інтегрує сучасні методи стратегічного аналізу, прогнозування, моделювання та оцінки ефективності управлінських рішень. Такий механізм має включати широкий спектр

інструментів, що охоплюють фінансове, виробниче, організаційне та інформаційне забезпечення процесу управління.

Таким чином, формування ефективного механізму стратегічного планування та управління сталим розвитком промислового підприємства є ключовим завданням сучасного управлінського процесу. Його реалізація сприятиме підвищенню конкурентоспроможності підприємств, забезпеченню їхнього довгострокового розвитку та адаптації до динамічних змін ринкового середовища.

1. Формування системи планування та управління сталим розвитком промислового підприємства.

Управління можна розглядати як складний і багатогранний процес, що здійснює цілеспрямований вплив на діяльність окремого працівника, групи людей або компанії в цілому. Його основна мета – досягнення оптимальних результатів, які відповідають певним критеріям та умовам. При цьому управління включає в себе не лише контроль за поточною діяльністю, а й стратегічне планування, організацію, координацію та коригування процесів, що відбуваються в межах підприємства чи організації.

Існують різні підходи до розуміння управління, і одним із ключових є трактування цього явища як процесу спрямованого впливу на керовану систему. Відповідно до такого підходу, управління полягає в переведенні системи з поточного стану в новий, наперед визначений, більш ефективний стан. Цей процес реалізується шляхом безпосереднього впливу системи управління на її ключові параметри, що забезпечує трансформацію в заданому напрямку (Польова, 2024).

Однак важливо зазначити, що управлінський процес не обмежується лише переходом системи до нового стану. Після досягнення бажаних змін виникає необхідність у підтримці отриманого рівня ефективності, що передбачає постійний моніторинг, аналіз і коригування діяльності у разі виникнення відхилень від запланованих показників. Таким чином, управління – це не статичний одноразовий акт, а динамічна система дій, спрямована на забезпечення стійкості та розвитку організації в довгостроковій перспективі.

Розглядаючи управління сталим розвитком, варто наголосити, що його найповніше визначення має містити такі ключові аспекти: управління сталим розвитком підприємства – це постійна, структурована та систематизована сукупність управлінських рішень та дій, які здійснює суб'єкт управління з метою впливу на об'єкт управління. Головне завдання такого впливу – забезпечення безперервного відтворення або збереження ефективного функціонування підприємства протягом визначеного проміжку часу.

Відтак, коли мова йде про управління сталим розвитком промислового підприємства, це передбачає не лише застосування окремих управлінських рішень, а й розроблення комплексної стратегії сталого розвитку, яка охоплює всі аспекти діяльності підприємства. Такий підхід є необхідною умовою для досягнення довгострокової конкурентоспроможності, оскільки дозволяє підприємству адаптуватися до змінних зовнішніх умов, мінімізувати ризики та ефективно використовувати наявні ресурси.

Детальний аналіз економічної ефективності та стабільного функціонування підприємств промислового сектору України свідчить про важливість формування єдиної, всеосяжної стратегії управління сталим розвитком. Ця стратегія має розглядатися як складна система, що включає в себе низку важливих елементів. До

таких елементів слід віднести визначення чітких цілей, формування відповідних завдань і принципів управління, розробку механізмів їх реалізації та встановлення показників оцінки ефективності.

Окрім цього, стратегічне управління сталим розвитком підприємства має враховувати не лише загальні принципи та методи управління, а й конкретні інструменти, які дозволяють реалізовувати визначені цілі. До таких інструментів належать організаційні структури, методики аналізу та оцінювання виконаної роботи, засоби управління ресурсами та кадровим потенціалом. Всі ці складові елементи взаємопов'язані між собою, а також перебувають у постійній взаємодії із зовнішнім середовищем. Саме ця взаємозалежність забезпечує можливість швидкого реагування на зовнішні виклики, ефективної адаптації до змінних умов та досягнення максимальних результатів в умовах конкурентного ринку.

Важливо зазначити, що створення стратегії управління сталим розвитком потребує ґрунтовного аналізу її ключових складових. До основних напрямів стратегічного управління можна віднести кілька важливих аспектів. Зокрема, це стратегія інноваційного розвитку, що спрямована на впровадження новітніх технологій і модернізацію виробничих процесів; стратегія соціального розвитку, яка включає в себе заходи з підвищення соціальної відповідальності підприємства, створення сприятливих умов праці та підтримки персоналу; а також стратегія зовнішньоекономічної діяльності, яка передбачає інтеграцію підприємства у світові ринки, розвиток міжнародного партнерства та залучення інвестицій.

Отже, управління сталим розвитком промислового підприємства – це багатовимірний процес, який охоплює різні рівні управлінської діяльності та потребує системного підходу. Його ефективна реалізація сприятиме підвищенню конкурентоспроможності підприємства, забезпеченню його економічної стабільності та створенню основи для довгострокового зростання.

Управління сталим розвитком поєднує в собі концепцію сталого розвитку та управління.

У науковій літературі частіше розглядається фінансова сталість підприємства, безумовно, найважливіша характеристика сталого розвитку. Однак при вивченні фінансової стійкості традиційно не говорять про управління фінансовою сталістю, хоча передбачається досягнення певних параметрів-характеристик (тобто деякі управлінські дії). Обговорюються принципи фінансової складової сталого розвитку підприємства. До них відносять: принцип усунення втрат (управляємо витратами), принцип подушки безпеки (формуємо резерви), принцип рентабельності вкладень - (підтримуємо ефективність), принцип відповідності (підтримуємо баланс оперативних і стратегічних потреб), принцип збалансованості ризиків (формуємо та керуємо «портфелем»). Деякі науковці (*Budnikevich, 2021*), розглядаючи принципи фінансового сталого розвитку підприємства, визначаються основні: цільова орієнтація, системність, комплексність. Зазначені принципи може бути визнано і принципами сталого розвитку підприємства. Також існує концепція (*Мануйлов, 2024*) використання загальних (наукова обґрунтованість, системність, модельованість, релевантність, мультиваріантність, співставність, вимірність) і специфічних принципів фінансової складової сталого розвитку підприємства: відповідність ресурсного потенціалу, інтелектуалізація ресурсного потенціалу, орієнтація на запити

системи управління, інноваційність організацій, кластеризація та віртуалізація організацій, випереджуюча інвестиційно-інноваційна активність.

Слід зазначити, що заявлені загальні та специфічні принципи сталого розвитку - це класичні принципи управління з «прив'язкою до місцевості», до певної функції - фінансовому управлінню.

Перелічені принципи фінансової складової сталого розвитку підприємства можна врахувати при формуванні принципів управління сталим розвитком - підприємства. Всі аналізовані принципи сталого розвитку певною мірою відображають сутність сталого розвитку, що визначається як сукупність трьох стовпів (екологічний, соціальний та економічний розвиток).

Деякими вченими досліджуються саме принципи сталого розвитку підприємства (Гречко, 2020).

Так, відзначені принципи управління сталим розвитком: орієнтація на продуктивний аналіз та реалізацію найбільш ефективних політик і стратегій, об'єднання науки і мистецтва управління та екологічної політики, забезпечення використання природних ресурсів, за умови невиснаження їх та збереження для подальших потреб.

Пропонуються одинадцять принципів сталого розвитку бізнес-системи підприємства: цінності, стратегія, цілепокладання, залученість, організаційна структура, клієнтоорієнтованість, система обліку, безпека праці, інфраструктура бізнес-системи, роль генерального директора, конфігурація бізнес-системи. Усі перелічені принципи дійсно важливі для оцінки та управління сталим розвитком підприємства, але потребують конкретизації, чіткого формулювання та логічного зв'язку саме зі сталим розвитком.

Існують дослідження принципів сталого розвитку виробництва (Principles of sustainable production) (Немашко, 2024), тобто, мова йде про виробничі підприємства. Тут описані дев'ять принципів сталого виробництва на основі концепції сталого виробництва: безпека продукції та упаковки, зниження відходів і побічних продуктів, економія енергії і матеріалів, зниження використання агресивних хімічних і фізичних агентів, оптимізація проектування робочих місць, оцінка та обговорення результатів процесу, ефективність праці, безпека. Автори в роботі запропонували свої одинадцять принципів сталого виробництва, ось деякі з них: проектування економіки замкнутого циклу, економія ресурсів і збереження їх цінності, раціональне управління відходами, пріоритет благополуччя співробітників, підвищення прихильності керівництва принципам сталого розвитку, сприяння співпраці зацікавлених сторін в ланцюжку створення вартості, вимірювання і оптимізація процесів сталого розвитку, збільшення використання стійких технологій. Зіставлення цих двох систем принципів сталого розвитку підприємства говорить про «узгодженість» понять та концепцій: однозначний пріоритет екологічної та соціальних складових сталого розвитку.

Провівши короткий огляд принципів сталого розвитку підприємства, запропонуємо авторський набір принципів (пропонований перелік принципів може бути розширений). Пропонуємо як принципи управління сталим розвитком підприємства розглядати дві групи принципів: загальні (такі як цільова орієнтація, системність, комплексність та інші) та спеціальні (які характеризують екологічний, соціальний та економічний розвиток). Докладно всі принципи перелічені у таблиці 1.

Таблиця 1. Принципи управління сталим розвитком підприємства

Принципи	Реалізація принципів управління сталим розвитком підприємства
Загальні принципи	
Цільова орієнтація, Системність, Комплексність, Наукова обґрунтованість, Модельованість, Релевантність, Багатоваріантність, Співставність, Вимірність.	Загальні принципи управління, як принципи управління сталим розвитком, добре відомі і не вимагають коментаря
Цифровізація	Розробка та реалізація цифрових та інформаційно-комунікаційних технологій
Інноваційність	Формування та реалізація програм інноваційного-збалансованого розвитку
Спеціальні принципи	
Стійкий екологічний розвиток підприємства	
Моніторинг індикаторів параметрів - навколишнього середовища	Формування та реалізація програм постійного контролю за екологічними показниками діяльності підприємства, моніторинг оцінки екологічного навантаження підприємства на довкілля
Формування та реалізація екологічної політики	Розробка та реалізація заходів щодо безпеки продукції, упаковки, виробництва, скорочення відходів; організація циркулярного виробничого процесу
Забезпечення використання природних ресурсів	Розробка та реалізація заходів щодо оптимального - використання природних ресурсів, максимального вилучення корисних речовин; організації утилізації поки що існуючих відходів
Сталий соціальний розвиток підприємства	
Орієнтація на запити споживачів, клієнтоорієнтованість	Розробка та реалізація заходів щодо формування програм удосконалення продукції та упаковки, можливого задоволення запитів споживачів
Безпека праці, оптимальна та безпечна організація робочих місць	Розробка та реалізація організації праці працівників, що сприяє високій продуктивності праці та збереженню здоров'я працівників
Благополуччя всіх співробітників	Розробка та реалізація програм організації соціального забезпечення (формування соціальної інфраструктури підприємства), організація своєчасної та відповідної оплати праці працівників,
Сталий економічний розвиток підприємства	
Відповідність ресурсного потенціалу	Розробка та реалізація заходів щодо оцінки та управління ресурсним потенціалом підприємства (основні засоби, оборотні, трудові ресурси)
Рентабельності вкладень	Розробка та реалізація заходів щодо організації рентабельної роботи, постійного контролю економічної ефективності діяльності
Формування резервів	Розробка та реалізація програм формування фінансових резервів на підприємстві, контроль та підтримання показників ліквідності

Загальні принципи сталого розвитку не потребують коментарів, вони загальновідомі та загальновизнані, але до складу загальних принципів включено нові принципи цифровізації та інноваційності.

Незважаючи на те, що цифровізація вже проникла у всі сфери діяльності, як принцип сталого розвитку розглядається порівняно недавно. Відзначимо, найважливіша роль цифрових та інформаційно-комунікаційних технологій у забезпеченні сталого розвитку сучасних підприємств за рахунок створення нових конфігурацій компонентів сталих моделей. «Сталі» підприємці впроваджують цифрові технології у свої бізнес-моделі, щоб використовувати створення соціальної та екологічної цінності. Цифровізація передбачає впровадження та використання цифрових технологій (хмарні обчислення, штучний інтелект, 3D-друк або мобільні обчислення та інші). Унікальні властивості цифрових технологій створюють цифрові можливості, але й створюють нові «цифрові» проблеми («висока вартість цифровізації», доступність інформації, надмірна відкритість, можливість цифрового шахрайства та інші).

Необхідно не забувати і про недоліки, протиріччя цифрової логіки та логіки сталого розвитку, «які ще необхідно вивчити». Тому процес цифровізації діяльності повинен сприяти сталому розвитку підприємства, хоча цей процес має бути контрольованим.

Досягнення стратегічних цілей сталого розвитку інтеграційних утворень – кластерів, визначається ендogenous здатністю до інновацій (що забезпечує економічне зростання) і підтримка корпоративної соціальної відповідальності (що забезпечує якість життя і збереження природного середовища) (Степаненко, 2020). Крім того, необхідно пам'ятати і про особливості нових сучасних продуктивних - інновацій - MVP (minimum viable product) - це мінімально життєздатний продукт, що передбачає ретельне опрацювання майбутнього ринку. В 42% випадків причиною - провалу стартапу стає відсутність ринкового попиту і мінімізація «бажаних» результатів (особливі управлінські технології). Адже є ще й особливі бережливі - інновації, в основі яких принцип максимальної економіки ресурсів: природних, - людських, фінансових і тимчасових, заснованих на дешевизні, якості та екологічності. Тому, інноваційність і інноваційна діяльність - найважливіша складова стійкого розвитку, але повинна досягатися дуже акуратно і економічно.

До основних факторів, які впливають на результативність управління сталим розвитком промислового підприємства, необхідно віднести:

- організацію управління сталим розвитком;
- рівень розвитку методів, засобів та інструментів управління сталим розвитком;
- якість проведення заходів щодо управління сталим розвитком.

Зазначимо, що недостатній прояв чи відсутність однієї чи кількох перелічених чинників може зруйнувати цілу систему управління сталим розвитком.

У загальну модель управління сталим розвитком необхідно включати такі основні елементи:

- формування підходів до управління сталим розвитком;
- прогнозування сталого розвитку;

- аналіз сталого функціонування;
- розвиток системи управління сталим розвитком підприємства.

Основними базовими методами управління сталим розвитком промислового підприємства є диверсифікація, ухилення від ризику, компенсація, локалізація та ін.

Резервування, дисипація, диверсифікація ризиків – найчастіше застосовні методи для промислових підприємств.

Розглянемо докладніше дані методи. Для початку розглянемо метод створення системи резервів, який аналогічний до страхування, проте зосереджений він у рамках самого підприємства. На підприємстві в даному випадку формуються страхові запаси матеріалів, комплектуючих і сировини, резерви коштів, визначається план їх розгортання в ситуації кризи, вільні потужності при цьому не задіяні, що передбачає встановлення як би про запас нових контактів і зв'язків.

Основою методу дисипації є розподіл загального ризику, що реалізується через об'єднання з різною часткою інтеграції з іншими підприємствами-учасниками, які мають зацікавленість у загальному успіху. При цьому підприємство отримує можливість зменшення своїх ризиків, залучаючи до вирішення загальних труднощів інші підприємства та іноді фізичних осіб як партнерів. Досягнення цієї мети промисловими підприємствами передбачає вступ до різних концернів, асоціацій, зокрема галузових, консорціумів.

Для підприємств, що об'єднуються, характерна як вертикальна інтеграція, що передбачає злиття компаній однієї галузі або одного підпорядкування для поділу господарських зон, з метою здійснення бажаної узгодженої цінової політики, так і горизонтальна, що передбачає об'єднання підприємств за послідовністю технологічних переділів, постачальницьких і збутових операцій. Таким чином, стає можливим досягнення додаткового ефекту, що полягає в тому, що на «вході» та на «виході» промислового підприємства відбувається створення зон передбачуваного товарного ринку, довготривалого надійного попиту та постачання ресурсів, необхідних для виробничого процесу та створення товарів. Зокрема, з'являється можливість диверсифікації загальних ризиків за періодами чи етапами реалізації стратегічних рішень.

Методи керівництва сталим розвитком промислового підприємства включає різні варіації диверсифікації:

- диверсифікацію діяльності, яка передбачає збільшення кількості готових до використання або вже використовуваних технологій, асортиментне розширення випуску продукції або послуг, що надаються, таргетування регіональних ринків тощо;
- диверсифікацію збутових ринків, що передбачає присутність на безлічі ринків з товарами та послугами одночасно, коли у разі провалу на одному існує можливість компенсації збільшення продажів на іншому, а також диференціація поставок між численними цільовими групами;
- різноманітність закупівель ресурсів, що передбачає взаємодію з різними постачальниками, що забезпечує зниження залежності промислового підприємства від навколишнього середовища, дає захист від ненадійності окремих постачальників ресурсів, матеріалів, комплектуючих, сировини.

Як напрямок зниження ризику настання загрозливих ситуацій, що пов'язано зі створенням способів і стратегій попередження небезпеки, можна назвати методи компенсації збурливих впливів. Дані методи на кшталт впливу є попереджувальними методами управління. Як правило, вони є більш трудомісткими, для їх здійснення потрібна велика попередня аналітична робота, причому ефективність застосування цих методів залежить від повноти та ретельності проведення аналізу та оцінки поточного стану підприємства. Стратегічне планування діяльності підприємства є найбільш переважним методом даного типу (Андрушкевич, 2024). Як засіб компенсації впливів, що збурюють, здійснення стратегічного планування дає ефект тоді, коли процес формування стратегії охоплює більшу частину сфер виробництва промислових компаній. Повноцінному стратегічному плануванню зазвичай передують аналіз та оцінка потенціалу підприємства, що дозволяють знизити невизначеність та передбачити виникнення негативних моментів у всьому виробничому ланцюжку. Таке вивчення потенціалу промислового підприємства передбачає завчасне визначення вузько профільних чинників сталого функціонування підприємства, і, дозволяє, заздалегідь розробити комплекс компенсуючих заходів, і навіть план використання та залучення резервів.

Сталий розвиток економіки промислового підприємства є наслідком та характеристикою якості прийнятих рішень. Реалізація стратегії сталого функціонування підприємства повинна відбуватися, перш за все, за допомогою розробки стратегії його сталого розвитку. Стратегічне управління є непростим багатофакторним процесом виконання різних стратегій, які, в результаті, передбачають наявність чіткого зв'язку з генеральною стратегією розвитку підприємства. Основним моментом в успішній діяльності підприємства є чітко сформульовані цілі та завдання в стратегії розвитку, що лежать в основі стратегії сталого розвитку підприємства, а також методи, за допомогою яких цілі втілюються в життя.

Стратегію управління сталим розвитком ми можемо побачити на рис. 1. і відповідно до нього виділимо основні етапи.

Починати процес управління сталим розвитком потрібно з визначення генеральної мети розвитку підприємства. Основною метою промислового підприємства в умовах невизначеності зовнішнього середовища є забезпечення його сталого розвитку, що передбачає такі загальні напрямки, як:

- підвищення господарської сталого розвитку підприємства;
- масштабна чи обмежена диверсифікація виробництва;
- підвищення конкурентоспроможності підприємства;
- переорієнтація чи зміна основної спеціалізації виробництва;
- підвищення якості продукції;
- скорочення виробничих витрат;
- організація виробництва нових видів продукції.

Далі слідує перший етап - аналіз фінансово-економічної діяльності підприємства. Цей етап дуже важливий для виявлення основних передумов розробки стратегії сталого розвитку.

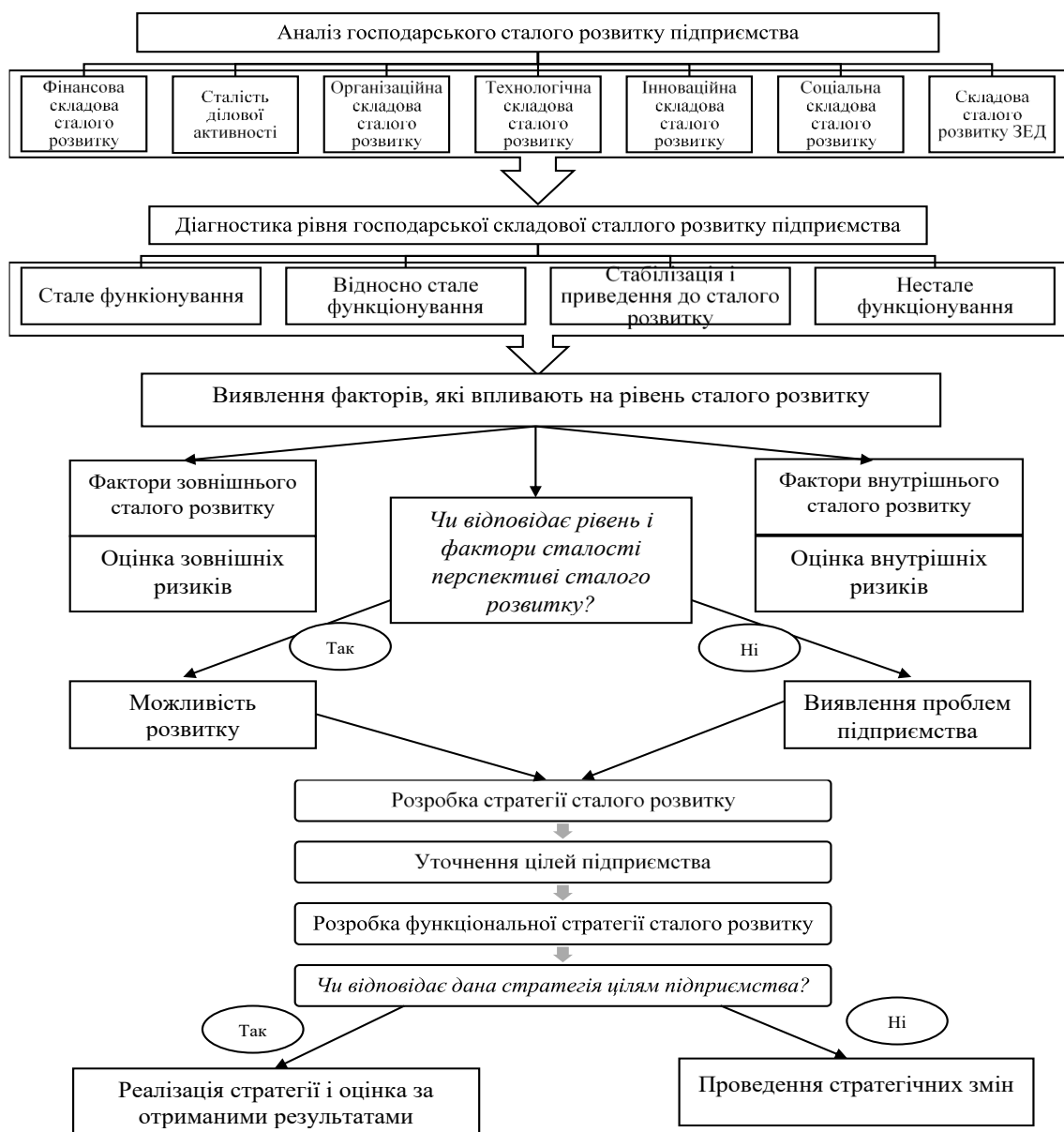


Рис. 1. Стратегія управління сталим розвитком промислового підприємства

Аналіз фінансово-економічної діяльності підприємства пропонується розділити на: аналіз фінансової складової сталого розвитку; аналіз сталості ділової активності; аналіз організаційного сталого розвитку; аналіз техніко-технологічного сталого розвитку; аналіз інноваційного сталого розвитку; аналіз сталого розвитку зовнішньоекономічної діяльності; аналіз соціальної складової сталого розвитку. При розробці стратегії сталого розвитку важливим є обґрунтування проміжку часу стратегії розвитку для вітчизняних підприємств, що є складним моментом, через складні непрості економічні умови, що характеризуються високою невизначеністю зовнішнього середовища, досить складним моментом стає прогноз розвитку

виробництва та підвищення його сталого функціонування (Шіковець, 2021).

Цей період значною мірою залежить від фінансового та економічного стану підприємства. Оскільки управління сталістю спрямоване на вдосконалення виробництва та розкриття економічного потенціалу підприємства, говорити про сталий розвиток доцільно тоді, коли для підприємства характерні:

- фінансова сталість;
- економічна стабільність (підприємство характеризується відносно стабільними економічними показниками);
- виробнича мобільність на діючих виробничих потужностях та наявність резервів їх використання;
- наявність певного ринкового сталого розвитку.

Головним першочерговим завданням формування стратегії управління сталим розвитком для вітчизняних підприємств стає фінансово-економічна стабілізація, яка робить можливим подальший сталий розвиток.

Враховуючи досить високий рівень нестабільності сучасної економічної ситуації в країні та високу ймовірність виникнення ризикових ситуацій для промислових підприємств, стає очевидним, що тимчасовий період має бути незначним. Однак це твердження не означає, що підприємствам не варто будувати свої плани на більш віддалену економічну перспективу.

На другому етапі передбачено діагностику віднесення результатів фінансово-господарської діяльності в одну з пропонованих зон сталого розвитку.

Цей етап необхідний для подальшого вибору загальної та функціональних стратегій сталого розвитку.

Щоб підвищити ефективність майбутніх рішень, на третьому етапі проведемо взаємозв'язок між показниками і коефіцієнтами, що дають характеристику компанії в результаті впливу зовнішніх і внутрішніх факторів на її сталість, і визначимо ступінь впливу даних на значення досліджуваних показників. Причому сукупність факторів зовнішнього і внутрішнього сталого розвитку слід розглядати як дестабілізуючі чинники, що впливають на підприємство.

На четвертому етапі керуючій ланці слід визначити, головні проблеми компанії та можливі шляхи вирішення цього кола проблем.

У ході п'ятого етапу топ-менеджерами розробляється стратегія підприємства, яка є базисом його сталого розвитку.

Шостий етап передбачає уточнення цілей підприємства. Оптимальним стає так зване «взаємопов'язане узгодження», тобто, коли процес розробки стратегії відбувається у взаємодії між вищим керівництвом, оперативними підрозділами планової служби. Вище керівництво встановлює цілі та напрями діяльності промислового підприємства. Формування стратегій відбувається у процесі взаємодії з вертикалі. Розробка таких практичних напрямів, як придбання, участь у нових проектах та спільних підприємствах, здійснюється відділом стратегічного розвитку на найвищому рівні управління підприємством.

На сьомому етапі розпочинається розробка функціональних стратегій. В результаті проведення у відповідності до розробленої методики оцінки сталого розвитку підприємства створюється підґрунтя для прийняття основних рішень, що

мають прямий зв'язок з формуванням та здійсненням поточного коригування функціональних стратегій сталого розвитку промислового підприємства під впливом на нього факторів зовнішнього та внутрішнього середовища.

Оперативні підрозділи виконують поставлені завдання вищого керівництва та самостійно формують функціональні стратегії розвитку та оперативні плани. Так, зазвичай стратегічні концепції на довгострокову перспективу розробляються на рівні підприємства, а середньострокові та поточні – оперативними підрозділами (виробничими відділеннями).

Заключним етапом є процес реалізації стратегії, який передбачає приведення в дію стратегії через розробку програм, підготовку бюджету та робочі процедури. Цей процес може зачіпати зміни загальної культури, структури та керівництва підприємства.

Етап оцінки та контролю є процесом, через який здійснюється моніторинг результатів поточної діяльності підприємства, щоб зіставити фактичну ефективність роботи з бажаним рівнем. Незважаючи на те, що оцінка та контроль реалізації стратегії є заключними елементами стратегії сталого розвитку підприємства, даний етап може забезпечити виявлення слабких місць у раніше реалізованих стратегічних планах, а також дати стимул до повторення всього процесу.

У процесі формування власних стратегій підприємство вибирає з альтернативних конкретні стратегії, які відповідають зазначеним орієнтирам управління, та адаптує їх стосовно власних особливостей. Зазначимо, що у процесі формування стратегії орієнтиром підприємства є прийнята вихідна концепція виконання цілей (Зомчак, 2022).

Розглянувши основні елементи розробленої стратегії управління сталим розвитком промислового підприємства, слід зазначити її універсальність.

У непростих умовах, у яких перебуває вітчизняна економіка нині, головною метою підприємств стає не тільки не припинення існування, а й формування передумов для подальшого перспективного прибуткового функціонування.

У сучасних умовах глобалізації економічного простору, що супроводжується активною інтеграцією світових ринків, прискоренням розвитком технологій та жорсткою конкуренцією з боку закордонних виробників, вітчизняним підприємствам дедалі складніше адаптуватися до динамічного середовища. Зміни у макроекономічних умовах, коливання валютних курсів, зміни у законодавчому регулюванні та нестабільність попиту – все це створює додаткові виклики для підприємств, які прагнуть забезпечити довготривале функціонування та розвиток.

За таких умов виникає нагальна потреба у формуванні чіткої та ефективної стратегії розвитку, що дозволила б підприємствам не лише залишатися конкурентоспроможними, а й активно розширювати свої можливості, нарощувати виробничий потенціал та мінімізувати можливі ризики. Однак розробка такої стратегії вимагає всебічного аналізу та ретельної діагностики рівня сталого розвитку конкретного підприємства. Проведення такої оцінки є важливим інформаційним інструментом, що дає змогу отримати об'єктивні дані про поточний стан компанії, визначити її сильні та слабкі сторони, оцінити наявні можливості та загрози, що існують у зовнішньому середовищі.

Відповідно, на основі результатів такого аналізу можна визначити першочергові

заходи, спрямовані на вдосконалення діяльності підприємства, усунення недоліків у функціонуванні та формування довгострокової стратегії сталого розвитку. Це, у свою чергу, дозволяє впроваджувати конкретні управлінські рішення, які допоможуть підприємству не лише стабілізувати свої показники ефективності, а й закласти основу для подальшого зростання та розвитку.

Оцінка рівня сталого функціонування є особливо важливою, оскільки дозволяє кожному підприємству обрати саме ту стратегію, яка найкраще відповідає його внутрішнім можливостям і зовнішнім викликам. Оскільки показники сталого розвитку можуть значно відрізнятись між різними підприємствами залежно від їхньої галузевої належності, масштабів діяльності, фінансового стану та конкурентного середовища, неможливо запропонувати універсальну модель, яка була б однаково ефективною для всіх. Саме тому кожне підприємство має формувати власну унікальну стратегію сталого розвитку, що відповідатиме його потребам та цілям, а також дозволить забезпечити стабільне зростання, навіть в умовах змінного зовнішнього середовища.

З метою впорядкування цього процесу та підвищення його ефективності доцільно розробити рекомендації щодо групування підприємств за рівнем їх сталого розвитку. Це дозволить чіткіше визначити пріоритети для кожної групи, запропонувати відповідні методи та інструменти для реалізації стратегій сталого розвитку. Такий підхід забезпечить системність у розробці стратегічних рішень і сприятиме їх практичному впровадженню.

Відповідно до запропонованого підходу, формування стратегії сталого розвитку має відбуватися в декілька етапів. Перший етап передбачає визначення загальної стратегії сталого розвитку підприємства, що дозволяє сформулювати основні принципи його довготривалого функціонування. На цьому етапі необхідно провести комплексний аналіз внутрішніх ресурсів підприємства, його ринкових позицій та можливостей подальшого зростання.

Після цього, на другому етапі, можна перейти до розробки функціональних стратегій, які охоплюватимуть окремі аспекти діяльності підприємства, такі як фінансовий менеджмент, інноваційна діяльність, екологічна відповідальність, соціальна політика тощо. Крім того, на цьому етапі варто розглянути конкретні рекомендації щодо впровадження та здійснення цих стратегій, що дозволить забезпечити їх ефективну реалізацію та досягнення запланованих цілей.

Однією з ключових стратегій сталого розвитку підприємства є стратегія зростання. Вона передбачає поступове збільшення масштабів діяльності, розширення ринків збуту, підвищення продуктивності та нарощування конкурентних переваг. Ця стратегія є найбільш доцільною для підприємств, які вже досягли певного рівня сталого функціонування та мають необхідні ресурси для подальшого розширення. Залежно від поточного стану підприємства стратегія зростання може реалізовуватися в абсолютному або відносному форматі, що означає або суттєве збільшення виробничих і фінансових показників, або поступове нарощування обсягів діяльності відповідно до наявних можливостей та зовнішніх умов.

Таким чином, формування та реалізація ефективної стратегії сталого розвитку вітчизняних підприємств є одним із ключових завдань сучасного менеджменту. Використання комплексного підходу, що базується на системному аналізі,

діагностиці та групуванні підприємств за рівнем сталого розвитку, дозволяє визначити найбільш релевантні управлінські рішення та забезпечити довготривалу ефективність їх реалізації (Ковальський, 2023).

Для реалізації базової стратегії сталого розвитку підприємство може зосередити зусилля на наступному:

- посилення присутності промислового підприємства на ринку;
- пошуку нових ринків збуту виробленої продукції;
- виході чи розширенні присутності підприємства на зовнішніх ринках;
- диверсифікації виробництва та освоєння нових видів продукції;
- підвищення вимог до посередників.

Стратегія стабілізації в якості стратегії сталого розвитку підприємства пропонується прийняти для реалізації підприємствам, для яких намітилася тенденція переходу від несталого до сталого функціонування, тобто підприємствам перехідної стабілізаційної зони. Такому підприємству потрібно прагнути до збільшення показника сталого розвитку, з метою переміщення з перехідної зони на наступний рівень - більш високу зону щодо сталого функціонування. Задля реалізації цієї базової стратегії підприємство може зосередити зусилля на:

- закріплення досягнутих ринкових позицій;
- випуск продукції за рахунок зміни застосовуваних матеріалів і ресурсів та діючих технологій;
- проведення заходів щодо скорочення витрат та втрат;
- запровадження інноваційних виробництв;
- підвищення автоматизації та комп'ютеризації існуючих виробництв.

Стратегія виживання в якості стратегії сталого розвитку підприємства пропонується до реалізації нестало функціонуючим підприємствам для уникнення великої ймовірності можливого банкрутства.

Підприємствам для поліпшення ситуації можуть бути запропоновані такі заходи:

- проведення моніторингу зарубіжних ринків з метою розширення збуту продукції, розширення кола покупців товару через його новизну або перевагу за цінами або якістю;
- комплексне вивчення зарубіжного ринку та адаптація виробництва до його вимог;
- удосконалення заходів щодо просування товару на закордонний ринок, розробка рекламної політики підприємства, орієнтованої на зовнішні ринки;
- створення власної інфраструктури зарубіжних продажів;
- підвищення якості продукції за допомогою застосування нових технологій, матеріалів, дизайнерських рішень;
- створення спеціального підрозділу у відділі ЗЕД
- розширення номенклатури вироблених для постачання на зарубіжні ринки товарів та послуг;
- продовження життєвого циклу продукції шляхом її реалізації на нових ринках, що характеризуються нижчим рівнем потреб та платоспроможного попиту;
- пошук нових зовнішніх каналів збуту продукції;

- мінімізація витрат виробництва та питомих витрат на одиницю продукції при оптимізації обсягів виробництва, що перевищують ємність внутрішнього ринку;
- використання спеціалізованого посередника з його торгово-збутовою мережею;
- вдосконалення процедур встановлення зворотного зв'язку із споживачами на зарубіжному ринку.

В основі стратегії сталого розвитку зовнішньоекономічної діяльності, націленої на задоволеність споживачів і отримання вигоди, знаходиться концептуальний підхід формування довгострокових конкурентних переваг економічного суб'єкта за рахунок оптимального поєднання ціни і якості виробленого продукту, здатності самого підприємства адекватно сприймати процеси змін (сигнали зовнішнього середовища), що відкривають для нього широкі можливості у зайнятті нових «ніш» (сегментів, областей, напрямів) на міжнародних (світових) ринках товарів, робіт, послуг. Ця стратегія передбачає послідовність дій та процедур, серед яких постановка цільових завдань зовнішньоекономічної діяльності підприємства; дослідження та визначення цільових зарубіжних ринків, розробку та реалізацію стратегій позиціонування товару, спрямованих на задоволення потреб споживачів цільових ринків. Така стратегія суб'єкта ЗЕД націлена не на реалізацію випадкових експортних можливостей, а на систематичну планову роботу з вивчення зарубіжних ринків і вибору найвигодніших серед них. При цьому основним завданням реалізації стратегії є пошук найбільш вигідних для підприємства способів та умов задоволення потреб ринку, виходячи з наявного внутрішнього потенціалу, а також формулювання напрямів розвитку останнього відповідно до прогнозованих змін зовнішнього середовища.

2. Механізм управління сталим розвитком промислового підприємства.

У сучасних умовах соціально-економічного розвитку механізм управління сталим розвитком поступово інтегрується в організаційну культуру підприємства. Це зумовлено тим, що він охоплює не лише економічні та управлінські аспекти, але й формує принципи та підходи до ведення бізнесу. Такий механізм поєднує в собі організаційні структури, методи управління та стратегічні орієнтири, які спрямовані на забезпечення довгострокової ефективності та відповідальності підприємства перед суспільством і навколишнім середовищем.

Процес створення ефективного механізму управління сталим розвитком має комплексний характер, включає роботу зі створення програми сталого розвитку. Механізм управління сталим розвитком залучає в цей процес всі ланки управління, починаючи від керівництва і закінчуючи працівниками, що підвищує ступінь досягнення намічених цілей сталого розвитку.

У процес управління сталим розвитком включаються керівники та фахівці, пов'язані з питаннями прийняття стратегічних рішень, які торкаються всіх сфер діяльності підприємства та стосуються всіх працівників. Під філософією ведення бізнесу ми розуміємо позицію підприємства в питаннях розвитку співпраці на внутрішньому і зовнішньому ринках, сформовані пріоритети в економічній діяльності, принципи побудови взаємовідносин з контрагентами, тощо. Це єдина система, що об'єднує місію, цілі та завдання стійкого розвитку підприємства, а також ідеологію, політику ведення бізнесу, діловий імідж та обмеження у підприємницькій діяльності, пов'язані зі сталим розвитком.

Таким чином, процес формування механізму управління сталим розвитком повинен ґрунтуватися на організаційній культурі підприємства, оскільки він є управлінським процесом. Реалізація цього процесу відбувається у кілька етапів.

1. Насамперед формулюється основна мета сталого розвитку, яка вибудовується на оцінці впливу стратегії на розвиток підприємства. Здійснюючи таку оцінку, фахівці можуть зіткнутися з деякими складнощами, у тому числі поєднання якісних і кількісних показників, встановлення їх розміру і фактичної величини, структуризація цільових значень і побудова дерева цілей, в якому вказується, вирішення яких підцілей веде до досягнення поставлених підцілей і сталого розвитку загалом. Тобто сталий розвиток підприємства не може бути досягнуто, якщо не реалізована хоча б одна підціль.

Специфіка діяльності підприємств, стадія життєвого циклу та інші фактори впливають на вибір та обґрунтування підцілей кожного з них, навіть якщо основна мета – сталий розвиток – збігається. Побудова дерева цілей має ґрунтуватися на скрупульозному аналізі діяльності підприємства, а також зовнішніх факторів, що впливають на його роботу. З іншого боку, враховується рівень сталого розвитку підприємства на ринку. Якщо становище підприємства нестабільне, розробляється дерево цілей із великою кількістю розгалужень, що дозволяють підприємству гнучкіше реагувати на вплив негативних чинників і мати більший вибір на формування стратегії. Чим стабільніше функціонує підприємство, тим менше гілок у дереві цілей йому необхідно для визначення шляху сталого розвитку.

2. На другому етапі проводиться розробка методів досягнення поставленої мети сталого розвитку. Для цього здійснюється аналіз проблем, що виникають, в результаті якого визначаються їх важливість, актуальність і пріоритетність, тобто проводиться ранжування проблем. Потім встановлюється вплив зовнішніх та внутрішніх факторів, визначається його характер, аналізується негативний вплив та його причини. Також оцінюється кількість і якість наявних у підприємства ресурсів, які можуть бути спрямовані на досягнення цілей сталого розвитку. Після складання експертного висновку з цих питань проводиться розробка кількох варіантів досягнення мети.

3. Наступний етап розробки механізму управління сталим розвитком передбачає вибір найбільш результативних шляхів подолання проблем підприємства на основі аналізу його життєвого циклу і наявних економічних і виробничих можливостей. Рішення про вибір варіанта розвитку підприємства приймається на базі існуючих міжнародних критеріїв та підходів.

Механізм управління сталим розвитком має цільовий характер, оскільки ґрунтується на постановці, виборі та реалізації цілей сталого розвитку. Дані цілі є рушійною силою для збільшення результативності економічної, соціальної, екологічної діяльності підприємства у стратегічній перспективі, дозволяють здійснювати координацію та контроль результатів функціонування, а також забезпечують прийняття ефективних управлінських рішень з питань сталого розвитку.

При цьому ефективність самого механізму управління сталим розвитком залежить від того, наскільки чітко визначені цілі та завдання сталого розвитку, наскільки правильно оцінені зовнішні та внутрішні фактори, що впливають на діяльність підприємства, а також наскільки правильно встановлено вектор розвитку.

Крім того, для розробки ефективного механізму управління сталим розвитком необхідно сформувати систему взаємопов'язаних між собою показників фінансово-господарської діяльності підприємства та показників його сталого розвитку, яка має бути підкріплена повною, достовірною, якісною інформаційною базою, що відповідає цілям та завданням сталого розвитку, що дозволяє приймати ефективні управлінські рішення.

На розробку результативного механізму управління сталим розвитком впливають різні чинники, які можна поділити на кілька груп (Ковальський 2023):

- фактори узгодженості механізму управління сталим розвитком із загальною стратегією розвитку підприємства, до яких відносять фактори ефективності досягнення цілей сталого розвитку, узгодженості методів та прийомів механізму управління з прогнозованою трансформацією зовнішньої обстановки, виникнення загроз сталому розвитку, зміни сегментарної кон'юнктури ринку тощо;

- фактори узгодженості механізму управління сталим розвитком із внутрішніми факторами підприємства, у тому числі наявним потенціалом розвитку, включаючи фінансовий, кадровий, організаційний, інформаційний та інші види потенціалу;

- фактори внутрішньої узгодженості механізму управління сталим розвитком, які передбачають баланс між конкретними цілями та цільовими показниками сталого розвитку, а також збалансованість у часі методів та прийомів досягнення поставлених цілей;

- фактори реалізації механізму управління сталим розвитком - дозволяють визначити можливість перетворення наявних у підприємства ресурсів для досягнення цілей сталого розвитку, а також залучення додаткових обсягів матеріальних та нематеріальних засобів з усіх потенційних джерел, використовуваних при цьому технології та економічні інструменти;

- фактори можливих ризиків при реалізації програми сталого розвитку – дають уявлення про рівень прогнозованих ризиків функціонування підприємства, а також їх допустимий рівень з позиції ймовірного виникнення економічних витрат з метою запобігання банкрутству;

- фактори ефективності досягнення цілей сталого розвитку, що ґрунтуються на загальних цільових завданнях розвитку підприємства.

Оцінювати ефективність механізму управління сталим розвитком ми пропонуємо відповідно до наступного алгоритму:

- 1) встановлення цілей оцінки, розробка параметрів та оціночних критеріїв, визначення джерел інформаційних даних для проведення оцінки;

- 2) формулювання питань, що вимагають вирішення в процесі оцінки, складання плану роботи, визначення використовуваних методів та прийомів оцінки, а також часу її проведення;

- 3) позначення конкретних показників, що визначають напрямки дослідницької роботи, що характеризують окремі параметри ефективності;

- 4) створення методичної карти, що включає методику та інструментарій формування інформаційної бази, вибір прийомів для знаходження взаємозв'язку між оцінюваними показниками;

- 5) розробка графіка проведення оцінки з визначенням її початку та закінчення, строків складання інформаційної бази, термінів надання проміжної інформації, а

також результатів оцінки;

6) формування бюджету проведення оцінки із зазначенням конкретних виконавців та співвиконавців, організаторів транспортного, інформаційного та іншого обслуговування, за рахунок накладних витрат;

7) узгодження цілей та завдань оцінки із замовником, затвердження витрат на її проведення, графіка та структури робіт, звітної документації;

8) основний етап - збір інформаційних даних, проведення їх аналізу, встановлення впливу окремих показників на ефективність механізму управління стійким розвитком, визначення взаємозв'язків та закономірностей, складання звітних документів;

9) порівняння отриманих в результаті оцінки даних з цільовими критеріями стійкого розвитку, формулювання відповідей на поставлені в ході оцінки питання в кількісному та якісному вираженні;

10) складання висновків відповідно до намічених цілей та підготовка рекомендацій після закінчення проведення оцінки, надання звітної документації замовнику та заінтересованим особам.

Дотримуючись запропонованої концепції сталого розвитку, що включає чотири компоненти, пропонуємо розкласти механізм управління сталим розвитком на кілька напрямків, що включають управління у сферах:

- економічної політики підприємства;
- соціальної політики;
- екологічної політики;
- зовнішньоекономічної (глобальної) діяльності підприємства.

Оцінка ефективності механізму управління сталим розвитком є аналітичним процесом, до якого залучаються як фахівці підприємства, так і експерти з питань сталого розвитку різних аналітичних агентств. Організація цього процесу заснована на методології та рекомендаціях, розроблених міжнародними організаціями, для відкритої звітності. Базою даних для оцінки можуть бути показники як сталого розвитку підприємства, так і його фінансово-економічної діяльності.

Експерти проводять аналіз якісного та кількісного впливу різних факторів зовнішнього та внутрішнього середовища на показники економічного, екологічного та соціального розвитку, а також розвитку зовнішньоекономічної діяльності підприємства. Для цього застосовується комплекс методичних прийомів, основними з яких є кореляційний та інтегральний методи аналізу, метод ланцюгових підстановок, методи програмування, евристичні методи, метод експертних оцінок тощо. Вибір певного методу аналізу залежить від завдань та цілей дослідження, його глибини та практичних можливостей реалізації.

Таким чином, дана оцінка дозволяє вирішити такі питання:

- об'єктивно відображає економічні, соціальні, екологічні та глобальні показники, що впливають на сталий розвиток підприємства;
- дозволяє порівнювати результати функціонування підприємства у поступовій динаміці, і навіть з результатами роботи інших підприємств.

Системний підхід до формування механізму управління сталим розвитком підприємства є об'єктивною необхідністю та обумовлюється взаємним впливом усіх складових частин механізму. У зв'язку з цим для формування ефективного механізму

управління сталим розвитком підприємствам необхідно керуватися такими положеннями:

1. Механізм управління - єдина система, що включає взаємозалежні елементи, що володіє властивостями цілісності, оптимальності, надійності, економічності, доцільності тощо.

2. Мета функціонування механізму управління стійким розвитком має бути чіткою, мати можливість для трансформації, визначатися на стадії його формування та забезпечувати концентрацію необхідних ресурсів.

3. Необхідне встановлення взаємозв'язків та схем взаємодії між елементами механізму та із зовнішнім оточенням.

4. Механізм управління має забезпечувати ефективність функціонування системи, що має перевищувати ефективність функціонування окремих елементів системи.

Впровадження та реалізація даних положень дозволить підприємству збільшити прибутковість діяльності, підвищити продуктивність, покращити соціальний та екологічний клімат на підприємстві, забезпечити розвиток зовнішньоекономічної діяльності.

Логічна модель механізму управління ефективним розвитком підприємства представлена на рисунку 2.

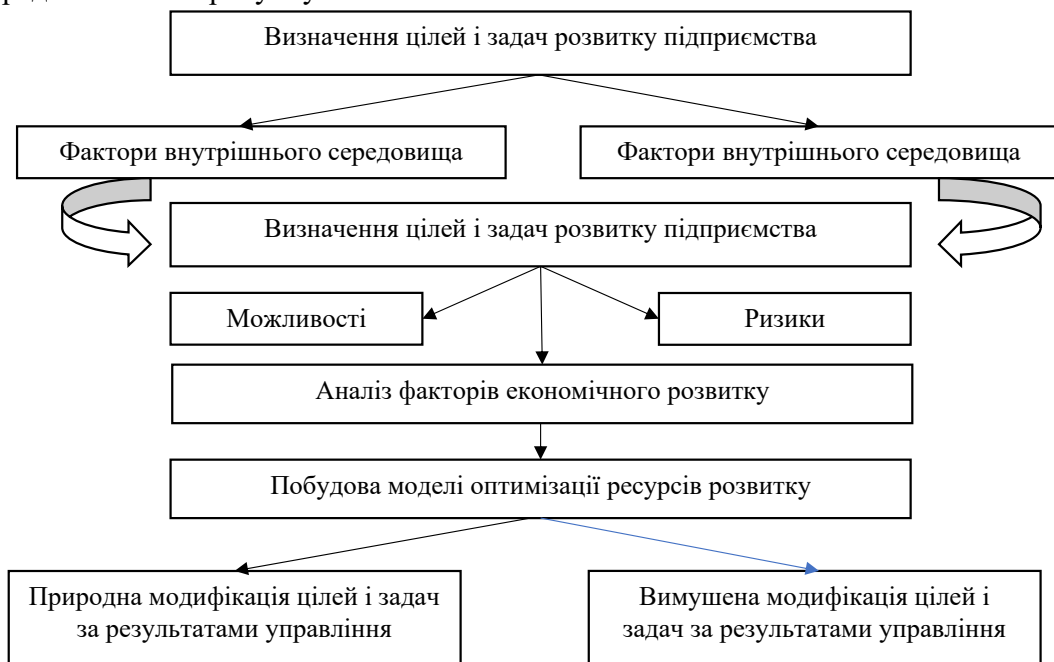


Рис. 2. Модель механізму забезпечення сталого розвитку промислового підприємства

Перший етап - це визначення цілей та завдань розвитку підприємства.

На другому етапі відбувається визначення підприємством чинників, які забезпечать ефективний розвиток підприємства. До зовнішніх факторів відносяться фактори зовнішнього макро- і мікросередовища, на які підприємство практично не може вплинути. До внутрішніх факторів належать фактори внутрішнього середовища, на які підприємство може безпосередньо впливати.

Ефективний розвиток промислового підприємства - це результат вмілого управління внутрішніми факторами, що зумовлюють результати діяльності підприємства. Забезпечення ефективності передбачає коригування факторів ефективного розвитку та побудову моделі оптимізації ресурсів розвитку.

Забезпечення сталого розвитку передбачає розробку алгоритму прийняття обґрунтованих управлінських рішень у різних управлінських підсистемах таким чином, щоб забезпечити керування факторами, що визначають сталий розвиток. Перед тим, як приймати управлінське рішення, необхідно оцінити рівень сталого розвитку на поточний момент, визначити фактори, що впливають на нього, та причини, вплив яких необхідно знизити.

При цьому визначення рівня сталого розвитку промислового підприємства має два основні призначення:

- теоретичне визначення сутності та змісту сталого розвитку підприємства;
- практична розробка та використання показників управління діяльністю підприємства для підвищення сталого розвитку.

Для гарантії сталого розвитку підприємства необхідно здійснювати діяльність за такими напрямками, щоб усунути причини нестійкого становища всередині підприємств:

- орієнтація ринку та конкуренцію;
- забезпечення прибутковості;
- зниження витрат;
- підвищення керованості та гнучкості організаційної структури;
- підвищення інвестиційної та інноваційної активності;
- створення механізмів зниження ризику втрат та ін. (Гасій, 2023)

Разом з тим, якщо розглядати сталий розвиток підприємства в цілому, то можна уявити два загальні напрями поступального розвитку підприємства:

- самозбереження підприємства, коли метою його діяльності є лише виживання, і відсутнє завдання стати лідером на ринку;
- саморозвиток підприємства, коли підприємство найбільш повно використовує виробничий потенціал, ресурси та націлене на збільшення обсягів виробництва та реалізації продукції, тобто, мета підприємства - сталий розвиток.

Таким чином, підприємство здатне працювати безвідмовно, забезпечуючи поступовий розвиток під дією доданих сил. Сила, яка забезпечує функціонування підприємства - це і є механізм забезпечення сталого розвитку підприємства, наявність якого є однією з основних ознак високорозвиненого підприємства.

Під механізмом управління сталим розвитком промислового підприємства розумітимемо систему, яка визначає порядок та зміст процесів, процедур, сукупність елементів і методів, організаційного забезпечення та інформаційних потоків, спрямованих на забезпечення можливості протидії негативному впливу ризикових факторів на діяльність підприємства з метою забезпечення сталого його розвитку.

Основними елементами механізму управління сталим розвитком промислового підприємства є способи реагування суб'єкта, який приймає управлінське рішення, на прояв ризикових факторів, що внаслідок визначає основні завдання представленого механізму у вигляді можливостей мінімізації ступеня прояву ризикових факторів на діяльність промислового підприємства.

Дія запропонованого механізму спрямована на обґрунтування вибору відповідних

стратегій та управлінських рішень з метою забезпечення сталого розвитку промислового підприємства з урахуванням його особливостей та напряму впливу ризикових факторів, ступінь прояву яких характеризують параметри відповідних індикаторів. Для досягнення цієї мети в рамках запропонованого механізму передбачено реалізацію низки взаємопов'язаних процесів, таких як: моніторинг параметрів зовнішнього та внутрішнього середовища підприємства (блок 1 на рис. 3); формування системи індикаторів оцінки сталого розвитку промислового підприємства (блок 2 на рис. 3); оцінка сталого розвитку промислового підприємства (блок 3 на рис. 3); розробка та прийняття управлінських рішень для забезпечення сталого розвитку промислового підприємства (блок 4 на рис. 3); розрахунок фактичних значень показників оцінки рівня сталого розвитку промислового підприємства (блок 5 на рис. 3); контроль результатів управлінських рішень, що приймаються (блок 6 на рис. 3). Взаємопов'язаний перелік процесів реалізації даного механізму дозволяє вирішити актуальне завдання забезпечення сталого розвитку промислового підприємства.

Дія механізму починається з моніторингу параметрів зовнішнього та внутрішнього середовища підприємства (блок 1 на рис. 3). Цей процес має передбачати не тільки проведення аналізу PEST-факторів на основі використання стандартних інструментів, але й бути орієнтованим на виявлення загального переліку ризикових факторів для промислового підприємства з урахуванням специфіки його діяльності. Для цього має бути використана інформація про зовнішнє та внутрішнє середовище підприємства. Такий моніторинг може здійснюватись співробітниками економічного відділу. Це залежить від особливостей організаційної структури підприємства та буде детально розкрито у рамках розробки організаційного забезпечення механізму управління сталим розвитком промислового підприємства.

Результати моніторингу параметрів зовнішнього та внутрішнього середовища підприємства дають змогу виявити загальний перелік ризикових факторів для промислового підприємства з урахуванням специфіки його діяльності. За своєю природою ризикові чинники діляться на внутрішні, природа яких визначається внутрішніми відносно підприємства чинниками, і зовнішні, які впливають на суб'єкт господарювання ззовні. У сучасній науковій літературі наголошується на необхідності управління ризиками, що виникають у процесі діяльності промислового підприємства (Пилипенко, 2020). Так, для промислового підприємства даний перелік включає наступні ризикові фактори: обмеженість ресурсів, антропогенні впливи, нераціональність використання ресурсів, прояв браку на різних стадіях технологічних операцій, порушення технологічних умов виробництва продукції, моральний і фізичний знос основних фондів, гостра нестача кваліфікованого персоналу, плінність кадрів, низька якість сировини та матеріалів, зміна коштів у часі, поява монополіста на ринку сировини та ресурсів можливість, неузгодженості дій між службами; посилення екологічних норм, стандартів та законів; неритмічність виробництва продукції та постачання ресурсів; неефективний розподіл робіт серед персоналу, шкідливі та небезпечні умови праці, підвищення ступеня автоматизації виробництва, конфронтація в колективі, висока конкуренція, витратоємний характер основної діяльності. Далі, у межах реалізації блоку 2 на рис. 3, дані ризики будуть деталізовані з урахуванням їх впливу на економічну, екологічну та соціальну сфери.

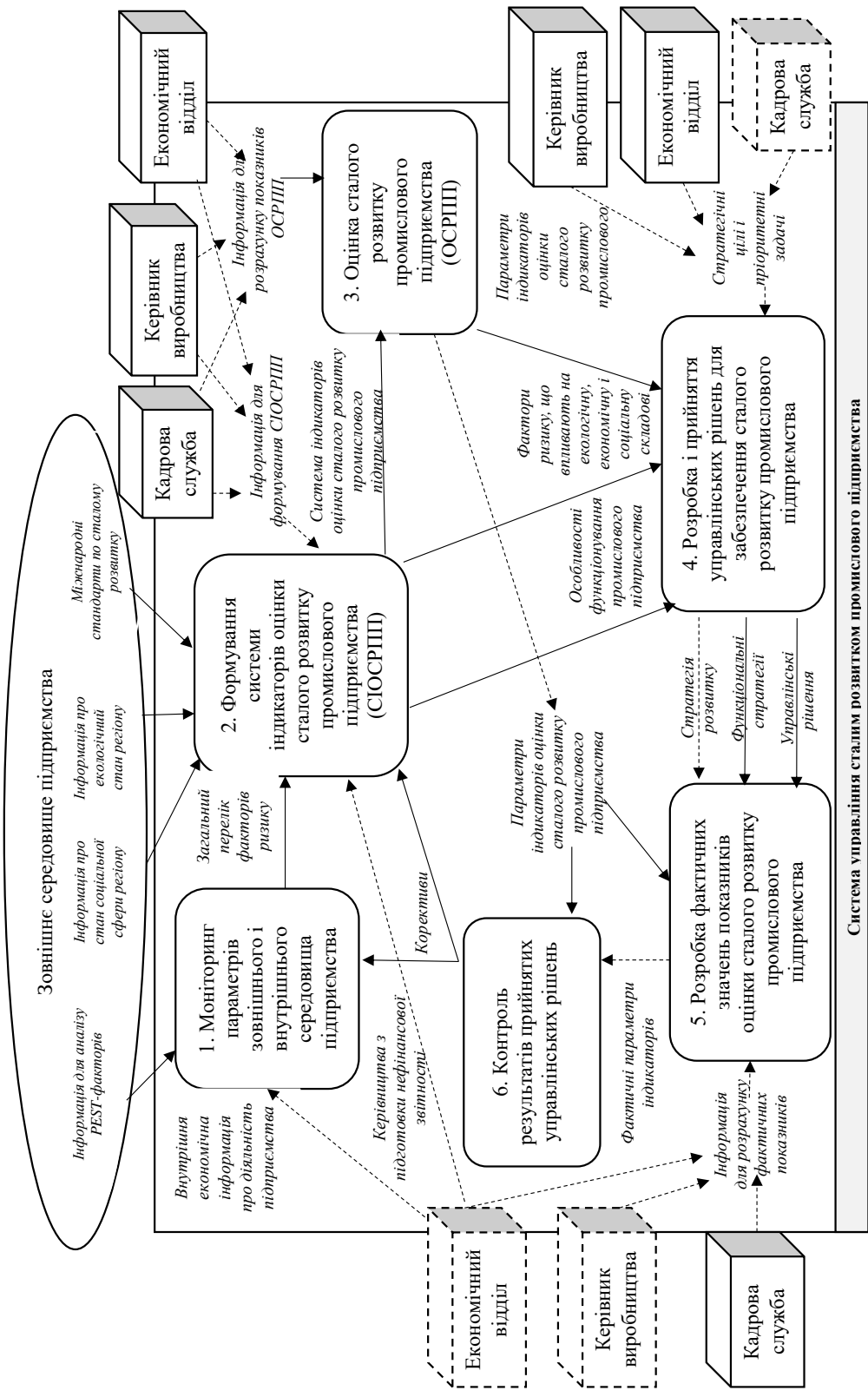


Рис. 3. Загальна схема механізму управління сталим розвитком промислового підприємства

Наступним, одним із особливо важливих процесів механізму управління сталим розвитком промислового підприємства є процес формування системи індикаторів оцінки рівня сталого розвитку промислового підприємства (блок 2 на рис. 3). Важливо при цьому враховувати зміст чинних міжнародних стандартів зі сталого розвитку, а також чинне керівництво з підготовки нефінансової звітності. Аналіз переліку показників, які рекомендуються з метою оцінки рівня сталого розвитку підприємств, свідчить про те, що вони переважно мають нефінансовий характер, характеризують соціальні, екологічні та економічні аспекти діяльності у їх взаємозв'язку. При цьому існує широке розмаїття даних показників, перелік яких подається у міжнародних стандартах та посібниках з нефінансової звітності без конкретизації у сферах діяльності підприємств. Складність і важливість цього процесу пов'язані з тим, що у практиці господарювання ще не сформувалося єдиної системи індикаторів оцінки рівня сталого розвитку промислового підприємства. Саме тому особливий науковий та практичний інтерес представляє можливість формування системи індикаторів оцінки рівня сталого розвитку промислового підприємства на основі використання інформації про стан соціальної сфери регіону, екологічну ситуацію в регіоні, а також загального переліку ризикових факторів, характерних для діяльності промислового підприємства. Для реалізації цього процесу співробітники кадрової служби, економічного відділу та начальник виробництва використовують відповідну інформацію, перелік якої буде деталізований у рамках розробки інформаційного забезпечення механізму управління сталим розвитком промислового підприємства.

Сформована у блоці 2 на рис. 3 система індикаторів оцінки сталого розвитку промислового підприємства може в подальшому коригуватися з урахуванням зміни вхідної інформації, а також, за необхідності, її зміни за результатами контролю. Маючи систему індикаторів та інформацію для розрахунку відповідних показників оцінки сталого розвитку промислового підприємства, відповідальні виконавці здійснюють розрахунки показників та виявляють ті індикатори, які сигналізують про необхідність ухвалення відповідних управлінських рішень з метою мінімізації ризиків зниження рівня сталого розвитку. На виході цього процесу визначаються конкретні параметри індикаторів оцінки рівня сталого розвитку промислового підприємства. Вони характеризують особливості його розвитку у певний період і є основою для подальшої розробки та прийняття управлінських рішень для забезпечення сталого розвитку.

Процес, що передбачений у запропонованому механізмі, охоплює розробку та прийняття управлінських рішень, які спрямовані на забезпечення сталого розвитку промислового підприємства. Цей етап є критично важливим, оскільки визначає стратегічний напрямок діяльності підприємства та способи його адаптації до мінливих умов зовнішнього середовища (блок 4 на рис. 3). Для ефективного впровадження цього процесу використовується широкий спектр інформації, що стосується ключових факторів ризику. Ці фактори безпосередньо впливають на три основні складові діяльності підприємства: екологічну, економічну та соціальну. Вони визначаються на попередньому етапі в рамках формування системи індикаторів оцінки сталого розвитку промислового підприємства (блок 2 на рис. 3). Аналіз і виявлення таких факторів є невід'ємною складовою управлінського процесу, адже саме вони дозволяють оцінити рівень ризиків і знайти ефективні шляхи їхнього

мінімізації. Крім того, для прийняття обґрунтованих управлінських рішень враховуються параметри індикаторів сталого розвитку, які були визначені на основі попередньої оцінки в блоці 3 на рис. 3. Ці параметри забезпечують підприємство актуальними даними щодо його поточного стану та допомагають визначити необхідні заходи для подальшого розвитку. Завдяки цьому управлінські рішення стають більш ефективними, оскільки базуються на об'єктивній оцінці реальної ситуації, а не на припущеннях чи загальних прогнозах.

Процес розробки та прийняття управлінських рішень у контексті забезпечення сталого розвитку підприємства викликає значний науково-практичний інтерес. Це пояснюється тим, що при його реалізації необхідно враховувати широкий спектр стратегічних цілей, а також визначені пріоритетні завдання підприємства. Оскільки кожне підприємство має свої особливості, варіативність стратегічних підходів у межах цього процесу є досить великою. Успішне управління неможливе без гармонійного поєднання стратегічного та оперативного рівнів прийняття рішень, що, своєю чергою, потребує використання комплексного підходу до управління.

3 цієї причини ефективна реалізація процесу розробки та прийняття управлінських рішень вимагає застосування науково-методичного підходу, який дозволить підприємству визначати оптимальні рішення, враховуючи не лише поточні потреби, а й довгострокові перспективи розвитку. Цей підхід має базуватися на комплексному аналізі зовнішнього та внутрішнього середовища підприємства, оцінці рівня ризиків та можливостей, а також на механізмах їхньої мінімізації та використання відповідних стратегічних інструментів. У результаті здійснення цього процесу, відповідно до інформації, представленій в блоці 4 на рис. 3, повинна формуватися або коригуватися загальна стратегія розвитку підприємства. Якщо така стратегія вже існує, то вона може зазнавати певних змін, уточнень або ж залишатися без змін, залежно від отриманих результатів аналізу та актуальних потреб підприємства. Аналогічно, розробляються та уточнюються функціональні стратегії розвитку підприємства, які визначають основні напрями діяльності у конкретних сферах – від виробничої та фінансової до екологічної та соціальної (Немашкало, 2024).

Крім того, на основі отриманих результатів приймаються відповідні управлінські рішення, які можуть стосуватися як короткострокових, так і довгострокових перспектив. Вони включають заходи щодо оптимізації бізнес-процесів, підвищення конкурентоспроможності підприємства, покращення ефективності використання ресурсів, впровадження інновацій та посилення соціальної відповідальності компанії.

Таким чином, процес розробки та прийняття управлінських рішень у межах механізму забезпечення сталого розвитку промислового підприємства є складним та багатоетапним. Він охоплює аналіз внутрішніх і зовнішніх факторів, визначення ключових ризиків, оцінку сталого розвитку, формування загальної та функціональних стратегій, а також прийняття рішень, які забезпечать стабільне зростання підприємства в довгостроковій перспективі. Ефективність прийнятих управлінських рішень може бути визначена за результатами розрахунку фактичних значень показників оцінки сталого розвитку промислового підприємства після реалізації керуючих впливів. Реалізацію цього завдання передбачено у межах процесу

розрахунку фактичних значень показників оцінки сталого розвитку промислового підприємства (блок 5 на рис. 1). Співробітники кадрової служби, економічного відділу та начальник виробництва надають необхідну інформацію для розрахунку фактичних показників оцінки сталого розвитку промислового підприємства.

Контроль результатів прийнятих управлінських рішень повинен здійснюватися за результатами зіставлення отриманих у блоці 5 (рис. 3) фактичних параметрів індикаторів з параметрами індикаторів оцінки сталого розвитку промислового підприємства, які визначалися до прийняття управлінських рішень у блоці 3 (рис. 3). Цей процес представлений у блоці 6 (рис. 3). За результатами його здійснення формується перелік необхідних коректив для подальшого проведення моніторингу зовнішнього та внутрішнього середовища підприємства та формування системи індикаторів оцінки його сталого розвитку. При необхідності внесення коректив цей механізм запускається знову з блоку 1 (рис. 3). Якщо за результатами контролю необхідність коректив не визначена, то процеси даного механізму здійснюються із встановленою керівництвом підприємства періодичністю. Якщо фінансово-економічна звітність формується підприємствами щокварталу, а також існують піврічні та річні форми звітності, то нефінансові звіти відповідно до міжнародних стандартів рекомендується формувати щорічно. Саме тому цей механізм пропонується запускати не пізніше, ніж у першому кварталі року, наступного за звітним, коли вже є вся необхідна інформація для реалізації процесів механізму управління сталим розвитком промислового підприємства.

Висновок. Для досягнення високого рівня ефективності функціонування та сталого розвитку в умовах недосконалої конкуренції необхідне перманентне забезпечення розвитку всіх сфер господарської діяльності у контексті критеріїв та принципів сталого розвитку. У рамках забезпечення цього процесу підприємству необхідно проводити оцінку, контроль, моніторинг, моделювання свого сталого розвитку, забезпечуючи при цьому комплексне, мультипланове застосування ендогенних факторів розвитку виробництва, інтегруючи та координуючи багатоаспектну діяльність окремих структурних одиниць організації у процесі здійснення виробничо-господарської діяльності.

Таким чином, розроблено механізм управління сталим розвитком промислового підприємства, який визначає порядок та зміст процесів, процедур, сукупність елементів та методів, організаційного забезпечення та інформаційних потоків, спрямованих на забезпечення можливості протидії негативному впливу ризикових факторів на діяльність підприємства з метою забезпечення його сталого розвитку. Особливістю даного механізму є можливість об'єднання між собою певної послідовності взаємопов'язаних процесів управління сталим розвитком промислового підприємства, розробка та прийняття управлінських рішень. Основною перевагою запропонованого механізму є можливість формування комплексного методичного забезпечення ефективного управління сталим розвитком промислового підприємства. В основу запропонованого механізму покладено принципи системного підходу, що дозволяє розглядати взаємозв'язок усіх процесів та їх виконавців, процедур, елементів, методів та інформаційних потоків, що дозволяє сформувати чітку послідовність дій, які необхідно здійснити для забезпечення сталого розвитку промислового підприємства. Формування системи індикаторів оцінки сталого

розвитку промислового підприємства представляє особливий науковий та практичний інтерес. Це завдання особливо актуалізується з урахуванням різноманіття існуючих показників, які рекомендуються міжнародними стандартами для оцінки сталого розвитку промислового підприємства. На окрему увагу також заслуговує вибір методики оцінки сталого розвитку промислового підприємства. Формування методичного, організаційного та інформаційного забезпечення запропонованого механізму управління сталим розвитком промислових підприємств є предметом подальших досліджень автора.

References:

- Зомчак Л., Коваль Л. Сталий розвиток регіонів України: просторово-панельний підхід. *Інфраструктура ринку*. 2022. Вип. 65. С. 211–215. DOI: <https://doi.org/10.32843/infrastuct65-35>
- Шіковець К. О., Квіта Г. М., Єрьоменко Я. М. Системно-ситуаційне моделювання цілей сталого розвитку. *Інфраструктура ринку*. 2021. Вип. 62. С. 102–107. DOI: <https://doi.org/10.32843/infrastuct62-18>
- Budnikevich I., Kolomytseva O., Rohozian Yu., Krupenna I., Zablodska D. Positioning of the amalgamated territorial communities of Ukraine through the sustainable development in the conditions of military actions. *Problemy Ekorozwoju*. 2021. Vol. 16, № 1. pp. 103–112. DOI: <https://doi.org/10.35784/pe.2021.1.11>
- Андрушкевич Н. В., Гнатюк О. П., Катана В. В. Особливості стратегічного планування і прогнозування підприємницьких структур. *Інвестиції: практика та досвід*. 2024. № 4. С. 154–160. DOI: <https://doi.org/10.32702/2306-6814.2024.4.154>
- Польова Н. М., Дубик Б. І. Теоретичні аспекти стратегічного планування в умовах цифровізації економіки. *Інвестиції: практика та досвід*. 2024. № 8. С. 131–140. DOI: <https://doi.org/10.32702/2306-6814.2024.8>
- Гасій О. В., Луцишин О. Ю., Кашкалда В. В. Сутність поняття «сталий розвиток». *Achievements of 21st Century Scientific Community: Proceedings of the 1st International Scientific and Practical Internet Conference*, September 14-15, 2023. FOP Marenichenko V.V., Dnipro, Ukraine, 523 p. С. 117–118. URL: <https://surl.li/rfngem>
- Гречко А., Очеретяна О. Дослідження еволюції наукової думки в аспектах визначення сутності поняття «сталий розвиток підприємства». *Підприємництво та інновації*. 2020. № 15. С. 37–41. DOI: <https://doi.org/10.37320/2415-3583/15.6>
- Степаненко Т. О. Теоретичні та методичні засади сталого розвитку підприємства. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Економіка і управління*. 2020. Том 31, вип. 70, № 6. С. 135–141. DOI: <https://doi.org/10.32838/2523-4803/70-6-23>
- Мануйлов О. В. Формування стратегії сталого розвитку підприємств в умовах невизначеності. *Український журнал прикладної економіки та техніки*. 2024. Том 9. № 2. С. 60–64. DOI: <https://doi.org/10.32782/2524-0072/2024-68-90>
- Ковальський А. Теоретичні аспекти формування стратегії сталого розвитку. *Економіка та суспільство*. 2023. Вип. 48. DOI: <https://doi.org/10.32782/2524-0072/2023-48-903>
- Немашкало К. Р., Хахалев Д. О., Мануйлов О. В. Методологічні підходи до управління сталим розвитком підприємства в умовах нестабільності. *Український журнал прикладної економіки та техніки*. 2024. Том 9. № 1. С. 365–371. DOI: <https://doi.org/10.36887/2415-8453-2024-1-62>
- Пилипенко С. М. Стратегічне управління підприємством на засадах концепції сталого розвитку. *Економіка та суспільство*. 2020. Вип. 21. С. 79–85. DOI: <https://doi.org/10.32782/2524-0072/2019-20-47>

CHAPTER 2. INTERNATIONAL COMMERCIAL ARBITRATION IN THE DIGITAL AGE: PROSPECTS AND INFORMATION SECURITY

Alla AVSIIEVYCH

PhD student, specialty D8 Law, Ph.D. Candidate

Educational and Scientific Institute of Law named after Volodymyr the Great,
Private Joint-Stock Company «Interregional Academy of Personnel Management»

taisha1878@gmail.com

<https://orcid.org/0000-0002-8192-8569>

Abstract. The article is dedicated to analyzing a relevant aspect of the modern legal landscape – the application of technological innovations in dispute resolution through international commercial arbitration. In particular, it examines the impact of the internet and digital technologies on shaping new approaches to conflict resolution. The relevance of this study is driven by the rapid advancement of technology and its integration into all sectors of the economy.

The growing interest in using online platforms for dispute resolution is attributed to their convenience and efficiency. The article highlights the key advantages of online dispute resolution, including speed, accessibility, cost reduction, and technological capabilities. At the same time, it explores the main challenges associated with such platforms, including technical aspects, security issues, and confidentiality concerns.

Special attention is given to factors influencing the effectiveness of online dispute resolution, such as the nature of the conflict, the level of cooperation between parties, and adherence to principles of fairness. A wide range of online platforms providing dispute resolution services is analyzed, along with their role in ensuring access to justice.

The study examines the practical aspects of using internet platforms, considering contemporary technological capabilities. The article also presents recommendations for the optimal use of online resources in legal practice. Successful cases of implementing such platforms in business, trade, and other industries are reviewed, along with an assessment of their potential adoption in Ukraine. Conclusions are drawn regarding the advisability of adopting foreign regulatory experiences for the effective operation of online dispute resolution platforms.

The article discusses issues related to the nuances of regulation and dispute resolution in cyberspace and concludes that the idea of abandoning offline dispute resolution methods in the near future may not be realized.

Keywords: arbitration, alternative dispute resolution methods, online arbitration, arbitration agreement.

МІЖНАРОДНИЙ КОМЕРЦІЙНИЙ АРБІТРАЖ У ЦИФРОВУ ЕПОХУ: ПЕРСПЕКТИВИ ТА ІНФОРМАЦІЙНА БЕЗПЕКА

Анотація. Стаття присвячена аналізу актуального аспекту сучасного правового простору – застосуванню технологічних інновацій у вирішенні спорів міжнародним комерційним арбітражем. Зокрема, розглядається вплив інтернету та цифрових технологій

на формування нових підходів до врегулювання конфліктів. Актуальність дослідження зумовлена стрімким розвитком технологій та їх впровадженням у всі сфери економіки.

Зростаючий інтерес до використання онлайн-платформ для вирішення спорів обумовлений їхньою зручністю та ефективністю. У статті висвітлюються ключові переваги онлайн-вирішення спорів, серед яких швидкість, доступність, зниження витрат і технологічні можливості. Водночас розглядаються основні виклики, пов'язані з використанням таких платформ, включаючи технічні аспекти, питання безпеки та конфіденційності.

Окрема увага приділяється факторам, що впливають на ефективність онлайн-вирішення спорів, зокрема характеру конфлікту, рівню співпраці сторін та дотриманню принципів справедливості. Аналізується широкий спектр онлайн-платформ, які надають послуги вирішення спорів, а також їхня роль у забезпеченні доступу до правосуддя.

Досліджуються практичні аспекти застосування інтернет-платформ з урахуванням сучасних технологічних можливостей. У статті також висувуються пропозиції щодо оптимального використання онлайн-ресурсів у юридичній практиці. Розглядаються успішні кейси впровадження таких платформ у сфері бізнесу, торгівлі та інших галузях, а також оцінюється потенціал їх запровадження в Україні. Зроблено висновки щодо доцільності перейняття іноземного досвіду регулювання онлайн-платформ для ефективного вирішення спорів. Розглядаються деякі аспекти досліджень щодо використання засобів альтернативного вирішення спорів, особливо використання електронного арбітражу, розглядаються питання, пов'язані з тонкощами врегулювання та вирішення спорів у кіберпросторі, і робиться висновок, що ідея відмови від офлайн-методів врегулювання спорів та вирішення спорів у найближчому майбутньому не буде реалізована.

Ключові слова: арбітраж; альтернативні способи вирішення спорів; онлайн-арбітраж; арбітражна угода.

Вступ. Стрімкий розвиток цифрових технологій призводить до їхнього проникнення у всі сфери життєдіяльності суспільства та держави. При цьому повсюдна інформатизація суспільства стає ефективним засобом реалізації прав громадян як в умовах диджиталізації, так і в ситуації, що сформувалась всесвітньою пандемією. Альтернативне вирішення спорів не стало винятком, і на сучасному етапі цифрові технології вже впроваджені в практику їх реалізації.

Онлайн вирішення спорів (далі – ОВС) (ODR, Online Dispute Resolution) – це цілий спектр методів, що виник з появою мережі Інтернет, і отримав новий імпульс для розвитку на тлі становлення електронної комерції та торгових майданчиків у мережі. У той самий час методи ОВС тісно пов'язані з методами АВС, до яких, зокрема, відносять третейський суд, арбітраж, медіацію та інші методи, що дозволяють знаходити позасудове рішення по спору.

Актуальність розгляду обраної для дослідження проблематики підтверджується, у тому числі, збільшенням кількості транскордонних угод, що здійснюються дистанційно, умовами пандемії, що, у свою чергу, породжує необхідність вирішувати спори/конфлікти, що виникають, без безпосередньої взаємодії сторін. Тобто це призвело до нової ери онлайн вирішення спорів.

Перш ніж перейти до розгляду чинних альтернативних механізмів, що ґрунтуються на застосуванні Інтернет-технологій, зазначимо, що сьогодні практично не має єдиної позиції у питанні щодо терміну, який слід використовувати при

визначенні таких АВС, наслідком чого виступають як термінологічна плутанина, так і різні проблеми вже у процесі розгляду конкретної справи.

В англomовній практиці використовуються наступні терміни:

- Інтернет-вирішення спорів (Internet Dispute Resolution – iDR);
- Електронне вирішення спорів (Electronic Dispute Resolution – eDR);
- Електронне альтернативне врегулювання спорів (Electronic ADR – eADR);
- Онлайн альтернативне врегулювання спорів (Online ADR – oADR);
- Онлайн-врегулювання спорів (Online Dispute Resolution – ODR).

При цьому останній із зазначених термінів є найбільш поширеним і усталеним, що доречно вживати тільки для складних систем вирішення спорів, тобто його застосування як мінімум некоректне для позначення будь-якого процесу електронного врегулювання спорів (наприклад, посередництво/переговори через Skype).

У сучасних умовах можливості цифрових технологій практично безмежні, що визначає допустимість їх використання як інструмента в межах будь-яких процедур – судових чи альтернативних.

Разом з тим, змішувати ці дві процедури при розгляді механізму врегулювання спорів онлайн представляється невірним, тому що ОВС не тотожно онлайн-судам та електронним інструментам, що використовуються в межах провадження в державних судах, що зумовлено публічно-правовим характером судової влади. Окрім цього, зарубіжні дослідники під час розгляду питань, пов'язаних з ОВС, безспідставно констатують наявність таких проблем, як відсутність єдиних стандартів належної правової процедури, а також механізмів забезпечення дотримання прийнятих рішень у разі їх невиконання у добровільному порядку (для вирішення цієї проблеми пропонується використання технології блокчейну).

1. Вплив інформаційно-комунікаційних технологій на розвиток електронної комерції та електронного арбітражу

Широке використання Інтернету в сфері міжнародної торгівлі призвело до появи нового її виду – електронної комерції. За визначенням Всесвітньої торгової організації (ВТО), електронна комерція – це «виробництво, розподіл, маркетинг, продаж або постачання товарів і послуг за допомогою електронних засобів зв'язку» (Декларація про глобальну електронну комерцію, 1998).

Інформаційно-комунікаційні технології (ІКТ) були створені з метою забезпечення оптимальних можливостей для передавання, обробки та збереження інформації. Завдяки можливості швидкої передачі й обробки даних вони сприяють ефективному альтернативному вирішенню спорів. Саме розвиток інформаційно-комунікаційних технологій передбачив появу електронного арбітражу.

Електронний арбітраж має кілька назв: Cyberation, Cyber Arbitration, Electronic Arbitration, Online Arbitration, Cyberspace Arbitration, Virtual Arbitration.

Міжнародний електронний арбітраж – це арбітражні процедури, що здійснюються через міжнародні канали комунікації в аудіовізуальній формі без необхідності фізичної присутності сторін спору та арбітрів у певному місці (*Цірат Г.А., 2019*).

Електронний арбітраж не відрізняється від традиційного арбітражу, окрім використання електронних засобів (Інтернету), за допомогою яких відбуваються

арбітражні процедури. Весь процес проходить в електронній формі без використання паперових документів і письмових приладь, а також без фізичної присутності сторін.

Електронний арбітраж починається із укладення електронної арбітражної угоди щодо передання спору, який вже виник або може виникнути в майбутньому, на розгляд міжнародного електронного арбітражу. Завершується процедура прийняттям електронного арбітражного рішення.

Порівняно з традиційним арбітражним розглядом міжнародний електронний арбітраж має низку переваг.

1. Швидкість вирішення спорів. Основною перевагою електронного арбітражу є оперативність у розгляді спору. Засідання сторін і допит свідків проводяться за допомогою електронних засобів зв'язку. Обмін документами та доказами здійснюється через електронну пошту або інші цифрові платформи, тоді як традиційний арбітраж вимагає особистої присутності сторін або їхніх представників. Миттєва передача інформації через Інтернет, телефонний зв'язок тощо дозволяє вирішувати спори протягом кількох днів, годин або навіть хвилин, що є особливо актуальним у сучасних умовах розвитку бізнесу (*Dispute settlement, 2003*).

2. Конфіденційність. Електронний арбітражний розгляд має високий рівень конфіденційності. Спори розглядаються у закритому форматі, що гарантує збереження комерційної таємниці. Цей аспект є вкрай важливим у міжнародних торговельних відносинах, укладених в електронній формі.

3. Подолання географічних обмежень. Використання інформаційно-комунікаційних технологій у процедурах вирішення спорів забезпечує доступ до арбітражу навіть у віддалених регіонах і для осіб з обмеженими фізичними можливостями. Електронний арбітраж сприяє вирішенню спорів у географічно ізольованих районах або у випадках, коли сторони не бажають зустрічатися особисто. Це ж стосується свідків та експертів, чиє фізичне прибуття не є обов'язковим.

4. Зниження витрат. Міжнародний електронний арбітраж є фінансово вигіднішим, ніж традиційний арбітраж. Відсутня потреба у тривалих і дорогих відрядженнях – сторони можуть брати участь у процесі з будь-якого місця, використовуючи комп'ютер, підключений до Інтернету. Це демонструє мобільність сучасного суспільства. Взаємодія через Інтернет дозволяє ознайомлюватися із заявами опонентів і надсилати документи у зручний для кожного з учасників час.

Отже, електронний арбітраж є ефективною альтернативою традиційному арбітражу, забезпечуючи швидкість, конфіденційність, доступність і економічну доцільність вирішення спорів.

5. Залучення професійних арбітрів. Важливою перевагою електронного арбітражу є можливість залучення фахівців, які мають досвід і визнану компетентність у сфері електронної комерції, а також технічних та правових аспектів такої діяльності. Сторони спору за взаємною згодою можуть обрати будь-який арбітражний орган і призначити арбітрів, яких вважають найбільш компетентними для вирішення конкретного спору. Як правило, це фахівці у сфері зовнішньої торгівлі, вузькопрофільні експерти з високим рівнем професіоналізму, незалежності та неупередженості. Кожна сторона обирає по одному арбітру, які, своєю чергою, призначають суперарбітра або головуєчого форуму.

Механізми електронного врегулювання спорів стали розглядатися як ефективна альтернатива національному судочинству та традиційному арбітражу. Зокрема, Окінавська хартія глобального інформаційного суспільства, ухвалена 22 липня 2000 року з метою підвищення довіри споживачів до електронних ринків, у пункті 7 рекомендувала розвиток «ефективних саморегулювних ініціатив: вивчення варіантів усунення складнощів, які виникають у споживачів під час транснаціональних спорів, зокрема через застосування альтернативних механізмів вирішення конфліктів» (*Окінавська хартія глобального інформаційного суспільства, 2000*).

Країнам, що розвиваються, було рекомендовано сприяти розвитку цих механізмів як альтернативи національній системі судового врегулювання спорів, щоб забезпечити довіру до нового ринкового простору. Також пропонувалося на законодавчому рівні стимулювати використання позасудових схем як ефективного способу вирішення конфліктів.

На сьогодні масштабні дослідження у сфері врегулювання спорів за допомогою мережі Інтернет проводять, зокрема, Центр інформаційних технологій та вирішення спорів (м. Амхерст, штат Массачусетс, США), Центр дослідження публічного права при Університеті Монреалю (Канада), Університет Лідса (Велика Британія), Міжнародний центр вирішення спорів при Університеті Мельбурна (Австралія), Факультет міжнародного приватного права та Центр інформатизації факультету точних наук Женевського університету (Швейцарія), Сінгапурська академія права (*Калаченкова К., Сінельник В., 2023*).

Значну роль у становленні електронного арбітражу відіграли такі електронні арбітражні центри, як «Virtual Magistrate» («Віртуальний суддя»), «CyberTribunal» («Віртуальне правосуддя»), Центр BOIV (Всесвітньої організації інтелектуальної власності).

Проект Virtual Magistrate («Віртуальний суддя») було створено у США в 1996 році Американською арбітражною асоціацією, Центром права та інформаційної політики Університету Вілланови та Інститутом права кіберпростору США.

За основу розгляду спорів у «Віртуальному судді» було вирішено взяти правила арбітражного розгляду Американської арбітражної асоціації. Вирішення спорів передбачалося проводити через Інтернет із використанням конфіденційних каналів доступу, що здійснювався за допомогою паролів.

Процедура врегулювання спору виглядала наступним чином:

1. Позивач заходив на сайт «Віртуального судді», заповнював електронну форму, де вказував інформацію про себе та опонента, описував суть спору та викладав свої вимоги.
2. Представники Американської арбітражної асоціації перевіряли заяву та визначали, чи потрібно надати додаткову інформацію.
3. Адміністратори сайту зв'язувалися з відповідачем, щоб отримати його згоду на участь у врегулюванні спору в рамках «Віртуального судді».
4. У разі згоди, представник Американської арбітражної асоціації допомагав сторонам правильно скласти арбітражну угоду.
5. Зі списку арбітрів обиралася особа, яка розглядала спір протягом 72 годин.

Юридична освіта не була обов'язковою вимогою для арбітрів, але вони повинні були мати достатній рівень знань у сфері права та інформаційних технологій. Усі арбітри зі списку «Віртуального судді» пройшли підготовку за спеціальною програмою, розробленою Американською арбітражною асоціацією для цього експериментального проєкту (*Al Ali Naser Abdel Rahim, 2021*).

Визнання та перспективи електронного арбітражу – проєкт отримав позитивні відгуки в Канаді, Великій Британії, Франції та Німеччині. Таким чином, було створено перший електронний арбітраж, що надав можливість вирішувати конфлікти у глобальній телекомунікаційній мережі Інтернет.

Розробники проєкту сподівалися, що:

- Інтернет-провайдери почнуть включати арбітражне застереження про розгляд спорів у «Віртуальному судді» до своїх договорів;
- Електронний арбітраж сприятиме створенню правил поведінки у віртуальному просторі, що призведе до формування прецедентного права кіберпростору.

Проєкт «CyberTribunal» («Віртуальне правосуддя») було запущено в червні 1998 року Дослідницьким центром публічного права юридичного факультету Університету Монреаля (Канада). Це був перший проєкт електронного вирішення спорів (ЕВС) за межами США, спрямований на врегулювання спорів, що виникають у сфері діяльності в Інтернеті, шляхом медіації та арбітражу.

За основу процедур було взято Арбітражний регламент ЮНСІТРАЛ. Розгляд справ здійснювався англійською та французькою мовами. Докази, як правило, надавалися в електронній формі. Однак за необхідності арбітр або медіатор міг досліджувати свідчення свідків та експертів, заслуховуючи їх особисто, телефоном або через відеоконференцію (*Арбітражний регламент ICC, 2012*).

«CyberTribunal» зробив значний внесок у становлення та розвиток ЕВС-руху в Європі. Проєкт активно співпрацював з низкою європейських організацій. Разом із Паризькою торгово-промисловою палатою та за підтримки Європейської комісії він знайомив торгово-промислові палати та бізнес-спільноти Брюсселя, Мілана, Рима та Копенгагена з процедурами врегулювання спорів через Інтернет. Також він взаємодіяв з науково-дослідними установами Бельгії, Німеччини, Франції та Іспанії з питань впровадження та подальшого розвитку ЕВС-механізмів.

Центр Всесвітньої організації інтелектуальної власності (далі – Центр ВОІВ) було створено у 1994 році під егідою Всесвітньої організації інтелектуальної власності (ВОІВ). Центр ВОІВ займається розглядом спорів, пов'язаних із інтелектуальною власністю, Інтернетом та електронною комерцією. Сьогодні Центр визнаний провідним постачальником послуг у сфері врегулювання спорів, що виникають при реєстрації та використанні доменних імен в Інтернеті (*Всесвітня організація інтелектуальної власності, 1994*).

3 грудня 1999 року по жовтень 2002 року Центр отримав 4500 справ, що стосувалися близько 8000 доменних імен, для розгляду за процедурою Єдиної політики UDRP. Центр також реалізує низку спеціальних проєктів, спрямованих на врегулювання спорів щодо загальних доменів верхнього рівня (.aero, .biz, .coop, .info, .museum, .name, .pro).

З кінця 2001 року спостерігається зростання кількості справ, поданих на розгляд до Центру шляхом арбітражу та медіації відповідно до Правил VOIB з арбітражу. Учасниками цих справ були спірні сторони з 13 країн на 3 континентах, а розгляд здійснювався англійською, французькою та німецькою мовами.

Тематика розглядуваних спорів включала:

- Договірні спори (наприклад, ліцензії на програмне забезпечення, дистриб'юторські угоди щодо фармацевтичних продуктів, контракти на науково-дослідні роботи).

- Недоговірні спори (наприклад, порушення патентних прав).

Крім того, Центр VOIB часто отримує запити щодо рекомендацій з вибору нейтральних експертів, а також може виступати призначаючим органом для експертів у випадках, коли сторони не є учасниками процедур VOIB, але потребують кваліфікованого арбітражного чи медіаційного розгляду, зокрема у сфері інтелектуальної власності.

Центр часто надає консультації з питань, що стосуються врегулювання спорів, пов'язаних з інтелектуальною власністю та мережею Інтернет, а також бере участь у розробці різних процедур для цих цілей.

Яскравим прикладом є процедура Єдиної політики (UDRP), яка базується на рекомендаціях, підготовлених VOIB щодо деяких зловживань у сфері доменних імен.

Аналогічно, у сфері електронної комерції, на запит Промислового консорціуму провайдерів прикладних послуг (ASPIC), Центр розробив набір перевірених практик для запобігання або вирішення спорів, спеціально орієнтованих на потреби провайдерів прикладних послуг (ASP) (Кравцов С., 2023).

Основними джерелами права, що регулюють питання міжнародного електронного арбітражу, є:

- Національне законодавство різних держав.
- Типові закони ЮНСІТРАЛ.
- Міжнародні договори.
- Арбітражна угода, укладена сторонами для передання спору до електронного арбітражу.

- Регламенти електронних арбітражів.

До таких регламентів належать:

- Онлайн-арбітражний регламент Китайської міжнародної економічної та торгової арбітражної комісії (08.01.2009).

- Турецький регламент про електронний арбітраж тощо.

Європейська конвенція про зовнішньоторговельний арбітраж 1961 року допускає використання електронних повідомлень, якщо це передбачено законодавством держав, представники яких уклали арбітражну угоду.

Не містять перешкод для укладання угод у електронній формі такі міжнародні акти, які діють лише на регіональному рівні:

- Брюссельська конвенція 1968 р. про юрисдикцію та примусове виконання судових рішень у цивільних і комерційних справах.

- Конвенція 1988 р. про юрисдикцію та виконання судових рішень у цивільних і комерційних справах.

- Регламент Ради ЄС № 44/2001 від 22.12.2000 р.

Відсутність бар'єрів у міжнародному праві (*Нью-Йоркська конвенція 1958 р., Європейська конвенція 1961 р., Арбітражний регламент ЮНСІТРАЛ*) та національному законодавстві створює сприятливі умови для розгляду арбітражних спорів із використанням електронних технологій.

Чинні міжнародно-правові акти та національне законодавство у сфері міжнародного комерційного арбітражу значною мірою обмежують можливість

- Розгляду спорів за допомогою електронного арбітражу.
- Представлення документів в електронній формі, що підтверджують згоду сторін на арбітражний розгляд.
- Вирішення питання підсудності (арбітражна угода, арбітражне застереження, третейський запис, пророгаційна угода).

Ці обмеження стримують розвиток міжнародного електронного арбітражу та вимагають суттєвих змін. Тому для правового регулювання електронного арбітражу необхідно:

1. Розробити та ухвалити під егідою ЮНСІТРАЛ Типовий закон про міжнародний електронний арбітраж.
2. Розробити та прийняти міжнародну конвенцію, що встановлює єдине правове регулювання міжнародного електронного арбітражу.
3. Вдосконалити як національне законодавство, так і арбітражні регламенти щодо електронної форми арбітражної угоди, арбітражного рішення, інших документів, підписаних електронним підписом.
4. Внести зміни до Нью-Йоркської конвенції ООН 1958 р. щодо визнання та виконання міжнародних електронних арбітражних рішень.

Основою функціонування міжнародного електронного арбітражу має бути електронна арбітражна угода – домовленість сторін про передання спору до електронного арбітражу.

ЮНСІТРАЛ у Типовому законі про міжнародний торговий арбітраж 1985 року (із змінами 2006 року) рекомендує тлумачити термін «письмова угода» таким чином, щоб він включав електронні повідомлення. У п. 4 ст. 7 зазначено:

«Вимога щодо укладання арбітражної угоди в письмовій формі виконується електронним повідомленням, якщо інформація, що міститься в ньому, доступна для подальшого використання. «Електронне повідомлення» означає будь-яке повідомлення, яке сторони передають за допомогою обміну даними. «Повідомлення даних» означає інформацію, підготовлену, відправлену, отриману або збережену за допомогою електронних, магнітних, оптичних чи аналогічних засобів, включаючи електронний обмін даними (ЕОД) – електронну пошту, телеграму, телексі або телефакс, але не обмежуючись ними».

Стаття 2 Нью-Йоркської конвенції 1958 року може застосовуватися до електронного обміну в різних формах, залежно від договірному процесу, прийнятого сторонами. Якщо договір укладається шляхом обміну електронними повідомленнями, ст. 2 може бути інтерпретована за аналогією. Крім того, судова практика вже визнала, що факсові копії та телексі є аналогічними листам і телеграмам. Отже, арбітражна угода є письмовою угодою, якщо вона була укладена шляхом обміну електронними повідомленнями.

Суть електронної арбітражної угоди полягає в тому, що вона фіксує волевиявлення сторін передати спір до міжнародного електронного арбітражу.

Ця угода надає міжнародному електронному арбітражу компетенцію розглядати спір.

Сторони повинні узгодити в електронній арбітражній угоді такі питання:

- Склад арбітражного суду.
- Мову провадження.
- Матеріальне право, яке застосовуватиметься для розгляду спору та ухвалення рішення.

Відповідно до Регламенту Арбітражного суду Міжнародної торгової палати в Парижі, Арбітражного регламенту ЮНСІТРАЛ та інших міжнародних арбітражних регламентів, сторони також можуть визначати власні правила вирішення спору та закріплювати їх в арбітражній угоді.

Визнання та виконання електронних арбітражних рішень

Конвенція ООН 1958 року про визнання та виконання іноземних арбітражних рішень, а також Арбітражний регламент ЮНСІТРАЛ 2010 року містять положення про те, що арбітражні рішення мають бути оформлені у письмовій формі.

Відповідно до п. 2 ст. 34 Арбітражного регламенту ЮНСІТРАЛ 2010 року:

«Усі арбітражні рішення викладаються у письмовій формі та є остаточними і обов'язковими для сторін. Сторони виконують усі арбітражні рішення негайно».

Хоча ці документи не містять прямих норм щодо проведення арбітражного провадження та ухвалення арбітражного рішення з використанням інформаційно-комунікаційних технологій (ІКТ), це не є підставою для відмови у визнанні та виконанні електронних арбітражних рішень.

Сьогодні технологічний розвиток відбувається в усьому світі та проникає в усі сфери життя. Здебільшого це спрямовано на забезпечення більшого процвітання та благополуччя: це зробило велику кількість людей здоровішими, їх життя комфортнішим та безпечнішим, ніж будь-коли в історії. Однією з таких технологічних трансформацій у сфері права є онлайн-вирішення спорів.

Онлайн-вирішення спорів, або ODR – Online Dispute Resolution (далі – ОВС) являє собою набір методів, який виник через розвиток інтернету і отримав новий поштовх завдяки розквіту електронної комерції та онлайн-торгових платформ. Варто зазначити, що методи онлайн-вирішення спорів тісно пов'язані з методами альтернативного вирішення спорів, як-от третейський суд, арбітраж, медіація та інші засоби, що дають змогу досягати урегулювання конфліктів поза судом (*Riikka K., 2016*). Застосування ОВС може поліпшити доступ до правосуддя, забезпечуючи швидший і менш витратний доступ до судів, що робить вирішення спорів більш ефективним і результативним. Проте широке використання ОВС також може обмежити доступ до правосуддя, створюючи технологічні бар'єри для всіх тих, хто не має можливості користуватися диджитал-технологіями. До того ж важливо звертати увагу на питання аутентифікації та ідентифікації сторін, цифрового бар'єру, кібербезпеки та захисту особистих даних (*Голубєва Н.Ю., 2021; Council of Europe, 1407 зустріч, 2021*).

Основними перевагами ОВС є: доступність – процес вирішення конфліктів доступним для широкого кола людей, незалежно від їх фізичного місцезнаходження,

це особливо важливо в умовах віддалених регіонів чи в ситуаціях, коли фізичний доступ обмежений; швидкість та зручність – онлайн-формат дає змогу швидко організувати розгляд спору, зменшуючи час очікування і робить процес більш ефективним. Учасники можуть брати участь у сесіях, не виходячи з дому чи офісу, що значно полегшує їхню участь. Проте під час вирішення спору онлайн можуть виникнути певні труднощі, зокрема, технічні питання – залежність від технічних засобів може викликати труднощі для деяких учасників, особливо тих, хто не має високого рівня комп'ютерної грамотності чи доступу до стабільного інтернету; безпека та конфіденційність – забезпечення конфіденційності та безпеки інформації під час онлайн-вирішення спорів є завданням, важливим для вдалого проведення. Важливо враховувати та використовувати заходи для захисту даних.

Варто наголосити, що для забезпечення справедливого вирішення спорів варто розробити відповідні та належні керівні принципи захисту прав людини під час використання ОВС. У країнах-членах Ради Європи ця вимога також впливає з гарантій, закріплених у Конвенції про захист прав людини й основоположних свобод, особливо із гарантій справедливого судового розгляду, що містяться в статтях 6 і 13 (*Конвенція про захист прав людини і основоположних свобод, 1950*).

Розвиток врегулювання спорів онлайн у країнах Європи призвів до прийняття у 2013 році нормативно-правових актів, що утворюють нормативну базу для врегулювання спорів онлайн, а саме: Директива 2013/11/ЄС Європейського Парламенту та Ради від 21.05.2013 р. про альтернативне вирішення спорів щодо спорів споживачів та внесення поправок до Регламенту (ЄС) № 2006/2004 та Директива 2009/22/ЄС (Положення про ODR споживачів) та Регламент (ЄС) № 524/2013 Європейського Парламенту та Ради від 21.05.2013 р. про вирішення спорів у зв'язку із споживчими спорами та внесення поправок до Регламенту (ЄС) № 2006/2004 та Директиву 2009/22/ЄС (*Калаченкова К. О., Сінельник В. І., 2023*).

Зараз на міжнародному рівні також діють Технічні коментарі ЮНСІТРАЛ щодо врегулювання спорів у режимі онлайн, прийняті 13.12.2016, які складені у формі документа, що описує елементи процедури врегулювання спорів у режимі онлайн. Важливо зазначити, що цей документ має рекомендаційний характер і створений відповідно до численних факторів, зокрема стрімкого збільшення кількості міжнародних угод, які укладаються в онлайн-режимі.

На жаль, інших міжнародних нормативно-правових актів, які б регулювали порядок вирішення спорів в онлайн-середовищі, наразі не існує. Отже, сьогодні на міжнародному, європейському та національному рівнях існує незначна кількість ефективних стандартів у цьому напрямі.

Наразі в зарубіжних країнах існує велика кількість так званих постачальників ОВС (сервісів, платформ, вебзастосунків для вирішення спорів онлайн тощо). Лідером за обсягами застосування технології онлайн-вирішення спорів є США. Прикладом системи онлайн-вирішення спорів є механізм вирішення спорів на eBay, яка відома значним рівнем використання та вражаючими показниками успішності. Центр вирішення конфліктів eBay, також відомий як eBay Disputes Resolution Center, являє собою систему вирішення спорів в інтернеті (ODR) для учасників торгівлі на платформі eBay national – покупців та продавців. Ітон Катчем (Ethan Katsh) розробив першу версію онлайн системи вирішення спорів на eBay, яка за два тижні

від початку її функціонування вже обробила 200 справ через електронну пошту. З того часу ця система перетворилася в повністю автоматизовану платформу, яка щороку вирішує до 60 мільйонів спорів.

eBay Resolution Center є невід'ємною частиною вебсайта електронної торгівлі eBay. До того ж на eBay надається гарантія повернення грошей, що може слугувати прикладом приватного механізму примусового вирішення спорів через систему ОВС (Rabinovich-Einy O., Katsh E., 2014). Платформа ОВС активна на всіх мовах Європейського Союзу з 15 лютого 2016 року та підтримується Європейською комісією. Найяскравішим прикладом постачальника ОВС, що довів свою ефективність, є Youstice, заснована у Братиславі (Словаччина), яка розпочала свою роботу у 2014 році як вебзастосунок для вирішення спорів в інтернеті. Ця платформа спрямована на обробку великих обсягів скарг споживачів із низькою вартістю, що стосуються як товарів, так і послуг, незалежно від того, чи були покупки здійснені в інтернеті, чи у звичайних магазинах. У межах цього сервісу передбачено два методи вирішення спору. Перший метод включає переговори між продавцем та покупцем. Другий метод дає змогу споживачам, які не отримали задоволення від результатів переговорів, обрати нейтрального посередника із запропонованого списку, який має акредитацію від Youstice. Процедура вирішення спору охоплює такі кроки: споживач реєструється на вебсайті, подає претензію, вибирає тип проблеми, вказує вимоги до продавця та взаємодіє з ним через діалог. У випадку, якщо рішення не влаштовує споживача, і він прагне застосувати більш серйозні заходи, він може звернутися до нейтрального експерта для вирішення спору за допомогою відповідної заявки. Якщо продавець не дотримується рішення, ухваленого посередником, споживач повідомляє Youstice, яка може вжити примусових заходів, зокрема контакт із продавцем, і за необхідності – застосування санкцій. Хоча конкретний спектр примусових заходів не визначено, партнери Youstice зобов'язані укладати угоди та виконувати рішення у більшості випадків, з платформи та можливе погіршення репутації, – репутаційну санкцію (Rabinovich-Einy O., Katsh E., 2020).

У Бельгії розроблено електронну платформу Belmed. СМС – інформаційний ресурс щодо цивільного, комерційного посередництва і посередництва в Англії й Уельсі (Голубєва Н.Ю., 2021).

Також існують інші платформи з онлайн-вирішення спорів, як-от: Demander Justice, ODR.com, ODR Platform of the European Commission, Modria, Rechtwijzer, CyberSettle тощо. Важливо зазначити, що ефективність цих платформ може залежати від конкретного контексту і характеру спору.

Найчастіше вирішення спорів онлайн застосовується в ситуаціях, пов'язаних із доменними іменами. У багатьох країнах існують спеціалізовані недержавні арбітражні центри, які вирішують спори, пов'язані з доменними іменами, за допомогою альтернативної процедури розгляду спорів – Єдиного регламенту розгляду спорів про доменні імена та Правил Єдиної політики вирішення спорів щодо доменних імен, розроблених Всесвітньою організацією інтелектуальної власності з арбітражу та посередництва (ВОІВ) та прийнятих Корпорацією з управління доменними іменами та IP-адресами (ICANN) у 1999 році (*Rules for Uniform Domain Name Dispute Resolution Policy, 1999; The Uniform Domain Names Dispute Resolution Policy, UDRP, 1999*). Основу цих правил становить Паризька конвенція з охорони

промислової власності, зокрема стаття 10, яка стосується актив недобросовісної конкуренції. Система UDRP використовується для боротьби з недобросовісними підприємцями, які реєструють домени для отримання прибутку завдяки репутації провідних брендів. Арбітражні центри, що вирішують спори відповідно до правил UDRP, не є третейськими судами або міжнародними комерційними арбітражними судами, а виступають як позасудові альтернативні методи вирішення спорів. Однією з найбільш відомих організацій для вирішення доменних спорів є Центр з Арбітражу та Посередництва BOIV, який щороку розглядає понад 3 000 спорів. За їх даними, кількість цих спорів щорічно збільшується не менше ніж на 10 % (Понов С., 2019). Специфіка спорів, які є предметом розгляду центрів, визначає їх вирішення без безпосередньої очної участі сторін, зокрема без використання відеоконференцз'язку.

Здебільшого практика арбітражних центрів, які розглядають доменні спори за правилами UDRP, зводиться до застосування їх власних попередніх рішень. Це пов'язано з тим, що країни, які беруть участь у спорі, мають різне законодавство щодо захисту прав на товарні та послугові знаки. Однак дії, пов'язані з реєстрацією доменних імен та поданням позову, можна аналізувати в контексті положень Паризької конвенції.

Істотною перевагою процедури, окрім скорочених термінів, дешевизни, конфіденційності, а також вирішення спору висококваліфікованими професіоналами в цій галузі, є необмежена територіальна дія, тобто єдиний механізм вирішення спору про доменне ім'я забезпечується незалежно від того, де знаходиться реєстратор, власник доменного імені або заявник. Водночас розгляд спору у межах адміністративної процедури UDRP не перешкоджає розгляду справи в суді (Бевз Г.М., Петренко І.В., 2020).

Практика судових рішень у доменних спорах в Україні пройшла суттєві зміни. Починаючи з 2000-х років, на початкових етапах розгляду справ суди вказували, що, згідно з чинним законодавством України, Принципи та Правила, встановлені організацією ICANN, не є обов'язковими на території України. Однак відповідно до статті 7 Цивільного кодексу України, ці норми можуть розглядатися як звичай ділового обороту, прийнятий у міжнародній практиці, що регулює відносини з вирішення спорів, пов'язаних із делегуванням доменних імен. Згодом суди стали доходити висновку про необхідність застосування принципу найбільш справедливого та ефективного способу захисту (*Доменні спори: різниця між підходами у розгляді акредитованими установами по UDRP та українськими судами, 2016*).

Зараз, судова система в Україні, на жаль, обмежена законодавчими нормами і не так глибоко використовує UDRP, як цього потребує звичай ділового обороту. Водночас, уповноважені установи ICANN, які мають акредитацію для вирішення доменних спорів, докладно вивчають усі аспекти реєстрації та використання об'єкта спору, формуючи власні прецеденти для подальших справ, оцінюючи конкретні обставини.

2. Зарубіжний досвід використання цифрових інструментів при розгляді спорів арбітражними інституціями

Використання цифрових технологій у правозастосовчій діяльності стало масовим явищем. Вплив розвитку техніки та технологій на сучасне суспільство є беззаперечним і сприяє активному впровадженню цифрових технологій у сферу

приватної юрисдикції. Зростання рівня діджиталізації правозастосовної діяльності органів альтернативної юрисдикції є не лише внутрішньоукраїнською, а й глобальною тенденцією, що зумовлює необхідність вивчення її впливу на цю сферу. При цьому зарубіжні юрисдикції випереджають Україну в деяких аспектах впровадження цифрових технологій у діяльність комерційних арбітражних установ.

Проблемними при застосуванні цифрових технологій у комерційному арбітражі, на думку деяких учених, проблемними при вирішенні спорів є як цифрова фіксація прав учасників (різні способи цифрової ідентифікації сторін (*Варакіна О., Хітрих М., 2020*)), так і функціонування цифрових сервісів та штучного інтелекту.

Використання цифрових технологій викликає низку проблем, зокрема:

1. Модифікація процедури вирішення спорів.
2. Функціональні можливості технологій під час взаємодії сторін у міжнародному комерційному арбітражі.
3. Забезпечення кібербезпеки прав учасників міжнародного комерційного арбітражу.

Використання цифрових технологій при розгляді правових спорів у комерційному арбітражі стало традиційною практикою у цій сфері. Це зумовлено такими перевагами, як зручність та ефективність для сторін, арбітрів і працівників арбітражних установ; економія часу та людських ресурсів; безпека електронного документообігу, зокрема персональних даних учасників.

Ці фактори, на нашу думку, сприяли активному впровадженню цифрових технологій в адміністрування комерційного арбітражу. Навіть пандемія COVID-19, не викликала стресових ситуацій у сфері комерційного арбітражу, оскільки цифровізація вже дозволила забезпечити стабільну діяльність арбітражних установ.

Розглянемо деякі аспекти міжнародного досвіду цифровізації арбітражного процесу. Наприклад, в Швеції створено інформаційну платформу SCC PLATFORM, яка з вересня 2019 року забезпечує проведення всіх арбітражних розглядів Арбітражного інституту Стокгольмської торгової палати. SCC PLATFORM – захищена цифрова платформа для комунікації та обміну файлами між сторонами та трибуналом (*SCC PLATFORM: Guidelines for parties and arbitral tribunals latest revision, 2020*).

Особливості SCC PLATFORM:

- Безпечна передача документів (процесуальних постанов, подань, доказів тощо), тобто це своєрідний форум з допомогою якого сторони, адвокати та арбітри взаємодіють впродовж всього розгляду справ по суті.
- Автоматичне створення індивідуального «сайту» для кожного арбітражу на цій платформі, доступ до якого мають лише сторони арбітражу.
- Безкоштовне використання для арбітражів, зареєстрованих до 31 грудня 2020 року (через COVID-19).

SCC PLATFORM працює на базі HighQ – світового лідера у сфері цифрових юридичних рішень. Система сертифікована за ISO 27001 та відповідає стандарту SOC2.

Німецький арбітражний інститут також запровадив цифровізацію арбітражного процесу. Арбітражний регламент DIS встановлює, що всі письмові повідомлення передаються в електронному форматі (електронною поштою, на цифрових носіях

тощо (ст.4); паперова передача допускається лише якщо електронний формат неможливий.

В Додатку 3 Арбітражного регламенту DIS як захід підвищення ефективності арбітражного розгляду зазначено можливість використання цифрових технологій у процесі (захист персональних даних, відеоконференції тощо). Формат використання цифрових технологій (обмін персональними даними, їх захист, обмін документами електронною поштою, аудіо-, відео-конференція) узгоджується з учасниками спору під час організаційного засідання та оформлюється процесуальним розпорядженням (*DIS Arbitration Rules, 2018*).

Результати діяльності постійно діючих інституційних арбітражів знаходять своє відображення у їх звітах чи розробці ними низки правил (регламентів), які стають обов'язковими для застосування, якщо сторони спору обирають той чи інший арбітраж.

Проаналізуємо підходи до організації розгляду справи провідними установами. Так, Міжнародною Торговою Палатою 9 квітня 2020 р. оприлюднені Керівні положення щодо можливих заходів, направлених на зменшення наслідків пандемії (далі – керівні Положення МТП 2020 р.) (*Guidance Note on Possible Measures Aimed at Mitigating the Effects of the COVID-19 Pandemic, 2020*).

У Керівних положеннях МТП 2020 р. розтлумачено, що можливість заслухати учасників арбітражного розгляду в контексті ст. 25(2) Арбітражного регламенту Міжнародної Торгової Палати (*Rules of Arbitration of the International Chamber of Commerce, 2017*) після розгляду всіх можливих клопотань і пред'явлення всіх необхідних доказів варто розуміти як безпосередню участь сторін спору, так і використання спеціальних технічних засобів для прийняття участі в «усному розгляді». Тож вирішення питання про можливість проведення розгляду справи в режимі відеоконференції має вирішуватися складом арбітражного суду в кожному випадку окремо з урахуванням усіх аспектів. І акцентуючи на визначенні дефініції «розгляд справи» Керівні положення МПТ 2020 р., визначають її як «живий, змагальний обмін між сторонами», який необов'язково повинен бути безпосереднім.

У 2020 р. Королівський Інститут арбітрів прийняв Типове Положення щодо дистанційного врегулювання спорів, яке враховувало сучасні рекомендації урядових та інших арбітражних установ у період пандемії COVID-19 або інших обставин, які б унеможливили проведення безпосередніх контактів сторін арбітражного розгляду. У Типових положеннях розкривається суть «дистанційного врегулювання спорів» крізь призму саме відео- та аудіоконференцій, хоча водночас передбачається, що такі форми проведення арбітражного розгляду є лише частиною цієї дефініції (*Guidance Note on Remote Dispute Resolution Proceedings, 2020*). Королівський Інститут арбітрів закликає сторони спору передусім використовувати комбіновані відео- або аудіоконференції, оскільки вони є більш ефективним засобом для врегулювання спорів у разі, коли розгляд справи з фізичною присутністю скасовується чи відкладається. Типові положення містять певні застереження, що стосуються дистанційного арбітражного розгляду. Оскільки різні країни мають різне законодавче регулювання та тлумачення норм щодо можливості дистанційного розгляду, виникають питання щодо визнання та виконання таких арбітражних рішень. Це може поставити під сумнів вибір такої форми проведення арбітражного розгляду.

Хоча цифрові технології набувають більшого визнання як комерційні та правові інструменти, існують такі застереження:

- сторони спору повинні усвідомлювати ризики застосування дистанційного формату арбітражного розгляду, включаючи можливість скасування арбітражного рішення або відмови у його визнанні та виконанні;

- сторонам спору рекомендується зберігати оригінали документів з підписами уповноважених осіб у паперовому вигляді. Це стосується як первісних документів (позов, договір, арбітражна угода тощо), так і всіх процесуальних документів, які можна отримати в арбітражі, якщо це можливо. Досить цікавим й дещо гнучким є погляд, що висвітлено у Звіті Бельгійського центру арбітражу та медіації «Усний розгляд під час COVID-19» (*Oral hearings in times of COVID-19, 2020*). Гнучкість полягає в тому, що, попри відсутність чіткої законодавчої регламентації щодо форм проведення арбітражного розгляду, у Звіті наведено поради для сторін спору та арбітрів щодо можливості вибору різноманітних варіацій розгляду справ при повному дотриманні права кожного бути заслуханим:

- дійсність. Немає потреби автоматично відкладати розгляд справи, щоб учасники спору могли бути фізично присутніми, оскільки віртуальні слухання здебільшого можуть вважатися дійсною альтернативою безпосереднім зустрічам.

- варіативність. Арбітражний розгляд не обов'язково має відбуватися виключно з фізичною присутністю учасників або бути повністю віртуальним. Комбіновані форми арбітражного розгляду дозволяють ефективніше й швидше вирішувати спори.

- можливість подання доказів. Якщо під час розгляду справи одна зі сторін хоче продемонструвати арбітрам доказ у паперовому вигляді, функція спільного використання екрану у віртуальному розгляді забезпечить арбітрам доступ до саме того доказу, на який звертає увагу сторона, чіткі та детальні процедурні правила. Склад арбітражного суду під час прийняття рішення про проведення дистанційного (віртуального) розгляду справи має чітко і зрозуміло визначити як організаційні (перевірка наявності технічної можливості, стійкий інтернет-зв'язок тощо), так і процесуальні аспекти задля запобігання виникнення проблемних питань (*Кравцов С., 2023*).

Для дослідження дефініції «віртуальний розгляд» в країнах континентальної Європи важливо надати аналіз Віденського Протоколу 2020 р. (Перелік передумов дистанційного розгляду), який розроблений та оприлюднений Віденським міжнародним арбітражним центром (Vienna International Arbitral Centre) та є керівними правилами для арбітрів і сторін спору щодо визначення того, чи є дистанційний розгляд справи доречним у конкретних обставинах (*The Vienna Protocol – A Practical Checklist for Remote Hearings*).

Обґрунтовуючи необхідність застосування Віденського Протоколу 2020 р., розробники зауважують, що ситуація з пандемією поставила сторони спору та арбітрів в умови, за яких вони вимушені шукати альтернативні форми безпосередньому арбітражному розгляду.

У тексті Віденського Протоколу 2020 р. зауважується, що через відсутність дозвільних та забороняючих норм щодо дистанційного розгляду в багатьох країнах світу за наявності лише абстрактного нормативного регулювання необхідно:

- розглянути питання про те, чи загалом допустимий дистанційний розгляд відповідно до закону місця проведення арбітражного розгляду та застосовних регламентів (якщо такі є);

- розглянути питання щодо виникнення потенційних проблем правозастосування під час дистанційного розгляду;

- у разі встановлення допустимості дистанційного розгляду розглянути питання доцільності призначення такої форми проведення розгляду спору в кожному конкретному випадку.

Як і більшість арбітражних регламентів, Арбітражний регламент Віденського міжнародного арбітражного центру 2021 р. (*Арбітражний регламент Віденського міжнародного арбітражного центру, 2021*) не містить чіткої норми щодо визначення та можливості вибору сторонами чи арбітражем чіткого виду арбітражного розгляду. У ст. 30 (1) Арбітражного регламенту 2021 р. передбачається, що: «..якщо сторони не домовились про інше, арбітражний суд ухвалює рішення щодо того, чи буде арбітражне провадження здійснюватися усно чи письмово.

Якщо сторонами не було виключено усне слухання, на прохання однієї з сторін арбітражний суд повинен провести таке слухання на відповідній стадії розгляду. З огляду на позиції сторін та конкретні обставини справи, арбітражний суд може прийняти рішення про проведення усного слухання за особистою присутністю сторін або за допомогою інших засобів. Сторони в будь-якому випадку повинні мати можливість ознайомитися з клопотаннями та поясненнями інших сторін та викласти суду свою позицію щодо них, а також щодо доказів» (*Арбітражний регламент Віденського міжнародного арбітражного центру, 2021*).

Отже, у цій нормі особлива увага зосереджується саме на можливості проведення «усного слухання», яке за своєю квінтесенцією наділене всіма ознаками дистанційного розгляду (*Цірат Г.А, 2019*). Таке твердження прямо узгоджується зі ст. 28 Арбітражного регламенту 2021 р., відповідно до якої «арбітражний суд має здійснювати арбітражний розгляд ефективно та з найменшими витратами відповідно до Віденських правил та угоди сторін, а в усьому іншому – на власний розсуд». Адже саме ці ознаки розгляду спору більшою мірою притаманні саме дистанційній, аніж безпосередній формі.

Попри таке диджитал-забарвлення арбітражного розгляду, на наш погляд, залишається все-таки невирішеним питання щодо врахування суб'єктивної думки сторін спору щодо можливості проведення дистанційного розгляду та співвідношення дискреційних повноважень арбітражу з «автономією волі» сторін спору.

Відповідь на ці два питання представлена у Рішенні Верховного Суду Австрії 2020 р. Так, арбітражний розгляд у цій справі проводився у Віденському міжнародному арбітражному центрі. У січні 2020 р. за клопотанням позивачів розгляд справи був відкладений на 15 квітня 2020 р., але через ковідні обмеження арбітрами в режимі відеозустрічі зі сторонами запропоновано проведення розгляду справи з використанням технічних засобів. Сторони спору заперечували проти проведення розгляду справи в такому форматі, подавши відповідні заперечення та прохання відкласти його на більш пізніший строк (*Guidance Note on Remote Dispute Resolution Proceedings, 2020; Born, Gary B., Anneliese Day, Hafez Virjee, 2020*).

Арбітражний суд за 7 днів до проведення слухання відмовив у задоволенні таких заперечень і вирішив, що все-таки розгляд справи буде відбуватися саме в режимі віртуального слухання. Після розгляду справи сторони, висунувши клопотання про скасування арбітражного рішення, стверджували, що відбулося несправедливе проведення розгляду справи з порушенням процесуальних гарантій і нерівне ставлення до сторін через проведення віртуального розгляду справи і унеможливлення підготуватися до судового засідання. Усі доводи зводились до того, що проведення арбітражного розгляду в режимі відеоконференції не відповідало європейським принципам щодо справедливого судового розгляду, відповідно відбулося порушення ст. 6 ЄКПЛ. До того ж сторона відповідача стверджувала, що під час віртуальних слухань неможливо встановити достеменно, якими документами будуть користуватися свідки та чи може бути на них здійснений вплив з боку третіх осіб. Верховний Суд Австрії, відхиляючи всі заперечення відповідача, зауважив, що:

- арбітражний суд наділений широкими дискреційними повноваженнями щодо управління арбітражним розглядом;

- справедливе й неупереджене ставлення до сторін спору не означає, що обидві сторони рівною мірою зобов'язані приймати участь під час розгляду справи, а лише те, що вони повинні мати справедливу потенційну можливість зробити це. Через те, що сторони були попереджені за 4 місяці до початку проведення судового засідання, то відповідно в них було достатньо часу для того, щоб підготуватися до нього;

- відеоконференція є загальновизнаним та широко поширеним інструментом проведення як арбітражних, так і державних розглядів, особливо під час пандемії. Отже, проведення віртуального слухання через відеоконференцію не порушує ст. 6 ЄКПЛ, оскільки має елементи права на доступ до суду, яке тісно пов'язане з правом на ефективний правовий захист;

- віртуальне слухання, що проводиться через відеоконференцію, може заощадити кошти та час, що сприятиме зміцненню правопорядку та водночас зможе забезпечити здійснення справедливого судового розгляду. Зокрема під час пандемії технологія відеоконференцій дає можливість гармонійно поєднувати право сторін на ефективне відправлення правосуддя й право бути заслуханим, що також є проявом верховенства права (*Scherer M., 2020; Oberster Gerichtshof in Republik Österreich, 2020*).

В Україні арбітражні інституції (МКАС при ТПП України тощо) також активно застосовують цифрові технології: відеоконференції, онлайн-засідання, електронний документообіг, що свідчить про оптимізацію діяльності українського арбітражу та його поступову цифрову трансформацію.

Правові аспекти цифровізації арбітражу, а саме використання інформаційних технологій ставить перед науковцями та практиками питання: чи розглядати цифровізацію як появу нової категорії прав, зокрема цифрових процесуальних прав, чи як одну з форм реалізації традиційних прав через сучасні технічні засоби?

Перший підхід вказує на те, що технологічні інновації не лише переосмислюють традиційні права людини (*Chaduteau O., 2018; Dusseaux A., 2018*), але й формують нове покоління цифрових прав (*sui generis*) (*Larret-Chahine L., 2016*). Другий підхід полягає в тому, що цифрові технології є інструментом оптимізації вирішення спорів, вони мають відповідати принципам законності та пропорційності

(Cohen S., 2016). Обидва підходи доступу до механізмів вирішення правових конфліктів шляхом застосування цифрових технологій підкреслюють важливість таких юридичних гарантій, як: доступу до інформації про процес, участі у розгляді справи, захисту персональних даних учасників арбітражу.

Таким чином, можна констатувати, що арбітраж є гнучким механізмом вирішення приватноправових спорів. Переваги арбітражу в умовах цифровізації у порівнянні із судовим процесом стають ще більш вагомими (Waincymer J., 2012). В частині створення умов для реалізації прав сторін можна відмітити наступні переваги:

- гнучкість арбітражних правил та процедур. Сторони можуть адаптувати процедуру під свої потреби, наприклад, узгоджувати процедурний графік, переносити слухання, проводити їх онлайн;

- впровадження технологій – відеоконференції широко використовувалися в міжнародному комерційному арбітражі ще до COVID-19;

- постійна адміністративна підтримка – всі міжнародні арбітражні установи забезпечують неперервний супровід справ;

- діджиталізація – електронна реєстрація, діловодство paperless (усі документи обмінюються в електронному вигляді: показання свідків, докази, висновки експертів, процедурна кореспонденція). Це риса, яка до сих пір ще не притаманна багатьом національним судовим системам;

- економія часу та коштів – арбітраж є менш вартісною та більш швидкою альтернативою національним судам. Основна перевага пов'язана з тим, що немає таких звернень, які можуть тривати роками у багатьох внутрішніх судових системах із збільшенням судових витрат. Національні суди часто затягують процеси на роки, тоді як арбітраж дозволяє заздалегідь оцінити витрати та вирішити спір ефективніше.

Таким чином, арбітраж в умовах цифровізації надає більш широкий спектр можливостей для ефективного вирішення спорів, а гнучкість процедури дозволяє врахувати інтереси сторін арбітражу при дотриманні основоположних принципів правової системи.

За останні 5 років використання цифрових технологій продемонструвало позитивний ефект у роботі арбітражних інституційних установ які здійснюють адміністрування арбітражного розгляду спорів. Різноманітні інструменти які призначені для дистанційних слухань, автоматизацію процесів, цифрову комунікацію між сторонами суттєво впливають на зміст юрисдикційної діяльності, що, звичайно, позитивно впливає на її ефективність.

3. Перспективи використання інформаційних технологій у вирішенні спорів міжнародним комерційним арбітражем

Широке поширення укладання правочинів засобами Інтернет призвело до виникнення конфліктів кардинально нового типу. Вирішення таких спорів такого типу вимагає не лише технічних знань, але й швидких рішень, і саме потреба в уніфікації підходів до вирішення конфліктів такого роду призвела до створення *lex electronica* – системи норм міжнародного права, яка регулює відносини, пов'язані із укладанням правочинів в електронному середовищі.

В свою чергу електронна комерція викликала до життя і електронну форму вирішення спорів, що виникають з такого типу правовідносин - онлайн-арбітраж. Термін «онлайн-арбітраж» може мати декілька значень, але, на думку Ю.Д. Притики,

найчастіше «він використовується для позначення арбітражного розгляду, який проводиться з використанням технологій віддаленої комунікації між учасниками процесу» (Притика Ю.Д., 2018; Арбітражний регламент ICC, 2012). Цей вид арбітражу набуває популярності в різних правових системах через його ефективність, швидкість, якість та вартість.

Онлайн-арбітраж є повноправним методом незалежного, неупередженого та ефективного вирішення конфліктів, що виникають з договірних та недоговірних відносин, за допомогою електронних засобів передачі та зберігання інформації. Метою його застосування є швидке та економічне вирішення суперечки без звертання до формальних процедурних правил.

Онлайн-вирішення спорів також може означати використання механізмів альтернативного вирішення спорів засобами мережі Інтернет. Методи вирішення спорів онлайн можуть бути використані для вирішення спорів, пов'язаних як офлайн, так і онлайн. Ідея використання механізмів альтернативного вирішення спорів «онлайн», а не «офлайн», виникла в 1990-х роках (Colin R., 2002. Ethan, K., 2004). Протягом цього десятиріччя деякі з найпомітніших послуг вирішення спорів онлайн надавали Проект «Віртуальний магістрат», Онлайн-офіс омбудсмена та Проект онлайн-медіації (Almaguer A., 1998; E. Casey Lide, 1996). Ці проекти спочатку розроблялися під егідою різних установ, включаючи Американську арбітражну асоціацію і Національний центр автоматизованих інформаційних досліджень.

Ініціалізм «ABC» який зазвичай помилково називають акронімом від «альтернативне вирішення спорів», був запропонований професором Гарвардської школи права Френком Е. А. Сандером (Frank Sander, 1985). ABC, простою мовою означає ідею врегулювання та вирішення спорів за допомогою різних засобів, відмінних від судового розгляду. ABC охоплює низку онлайн-засобів зв'язку, включаючи «електронну пошту, інтернет-ретрансляційний чат, обмін миттєвими повідомленнями, обговорення на веб-форумах та подібні текстові електронні комунікації».

За короткий проміжок часу фахівці з вирішення спорів зрозуміли, що існують можливості для значного розширення цієї галузі, що розвивається. У 1997 році професори Ітан Катш і Джанет Ріфкін заснували Національний центр технологій і вирішення спорів, який «підтримує і підтримує розвиток додатків інформаційних технологій, інституційних ресурсів, а також теоретичних і прикладних знань для кращого розуміння і управління конфліктами» (Andrew Pirie, 2000). Через чотири роки була написана перша книга в галузі ABC (Ethan Katsh, 2001). Пізніше сферу ABC почали досліджувати такі установи, як Федеральна торгова комісія США, Міністерство торгівлі США, Гаазька конференція з міжнародного приватного права, Організація економічного співробітництва та розвитку, Глобальний діловий діалог, Всесвітня організація інтелектуальної власності та Європейський Союз. Зокрема, в Європейському Союзі законодавчі заходи, як правило, сприяють використанню механізмів ОВС. Прикладами можуть служити Директива про електронну комерцію, стаття 17, і Директива про деякі аспекти медіації в цивільних і комерційних справах, Декларації 8 і 9. Крім того, у сфері споживчого права було прийнято як нову Пропозицію щодо Положення про онлайн-вирішення спорів щодо споживчих спорів, так і Пропозицію щодо Директиви про альтернативні способи вирішення спорів. Ці

пропозиції мають на меті покращити функціонування внутрішнього ринку роздрібної торгівлі та посилити відшкодування збитків для споживачів.

В принципі, очікується, що механізми ОВС, серед іншого, «полегшать доступ до правосуддя» (*Julio Cesar Betancourt, Elina Zlatanska, 2013*), а отже, повинні бути в змозі вирішити деякі проблеми, пов'язані з використанням офлайн-механізмів вирішення спорів. Вважається, що АВС може «вирішувати суперечки швидше й ефективніше», ніж традиційні методи, але, наскільки нам відомо, не було надійно та вміло проведено жодного дослідження, яке б підтверджувало це припущення. Науковці висунули різні пропозиції, спрямовані на розробку системи альтернативного вирішення спорів, і за останні 10 років було розроблено значну кількість послуг в цій сфері. У широкому спектрі механізмів АВС найбільш поширеними є переговори, посередництво та арбітраж.

Оскільки юридична професія почала модернізувати свою робочу практику за допомогою кількох технологічних досягнень у галузі обчислювальної техніки та телекомунікацій, можна задатися питанням, чи не буде зрештою використання офлайн-механізмів замінено використанням так званих механізмів АВС.

Електронні переговори є однією з найбільш поширених форм вирішення спорів і, ймовірно, однією з основних форм взаємодії. Вважається, що люди ведуть переговори, навіть якщо не думають про себе. Переговори, по суті, можна визначити як будь-який вид спілкування між двома або більше людьми з метою досягнення згоди. Для цього переговори можна розглядати як дружній і, можливо, дуже бажаний спосіб вирішення суперечок. З появою Інтернету ця форма взаємодії, особливо в сфері вирішення спорів та юридичної професії, дещо перемістилася з судових коридорів та відшліфованих офісів юридичної фірми в Інтернет, що призвело до просування ідеї переговорів на основі електронних переговорів (e-negotiation).

Перший дослідницький проект в області переговорів через Всесвітню павутину (INSPIRE) був введений в дію в 1996 році. Цей проект був розроблений у контексті крос-культурного дослідження процесу прийняття рішень та переговорів. Широкі експерименти з INSPIRE спонукали до розробки кількох інших систем електронних переговорів (*Julio Cesar Betancourt, Elina Zlatanska, 2013*). Ці системи разом із системами підтримки прийняття рішень були класифіковані за кількома категоріями, включаючи системи планування, системи оцінки, системи втручання та системи процесів. Однак поінформованість громадськості про ці засоби залишається дуже низькою, і тому ще належить з'ясувати, чи отримають переговори на основі електронних засобів, які покладаються на ці системи, широке визнання.

Поняття електронних переговорів нерозривно пов'язане з поняттям комп'ютерно-опосередкованої комунікації. Стверджується, що така комунікація полегшує процес взаємодії за допомогою комп'ютерів. Інтернет, без сумніву, став одним з основних засобів комунікації та обміну інформацією. Коротке текстове повідомлення (смс) через електронну пошту, наприклад, стає все більш звичним явищем. Вже десять років назад корпоративні користувачі відправляли і отримували приблизно 105 повідомлень електронної пошти в день, тобто 38 325 листів на рік. Потрібне нове дослідження, щоб визначити, скільки з цих повідомлень електронної пошти, якщо такі були, були пов'язані з якимись переговорами, але з точки зору ефективності електронних переговорів за допомогою електронної пошти це може

призвести до непорозуміннь, зловісних атрибуцій і, зрештою, до глухого кута переговорів.

Власне електронний арбітраж можна визначити як «електронну версію офлайн-арбітражу». Вона охоплює все: від арбітражної онлайн-угоди до арбітражного рішення онлайн. Взагалі кажучи, у світлі принципу автономії сторін обґрунтованість онлайн-арбітражу не є проблемою. Однак у міжнародному контексті було висловлено низку занепокоєнь щодо дійсності не лише онлайн-арбітражних угод, а й арбітражних рішень онлайн, особливо в розумінні Нью-Йоркської конвенції 1958 р. Ми можемо стверджувати, що ця Конвенція була прийнята «у той час, коли укладачі не могли передбачити, що [арбітражні угоди, арбітражні рішення] можуть набувати іншої форми, ніж фізична». Таким чином, можна лише припускати, що суди з часом погодяться з тим, що арбітражні онлайн-угоди та арбітражні рішення онлайн задовольняють формальним вимогам Нью-Йоркської Конвенції, і тим самим, не виникне в подальшому проблем з визнанням та виконанням іноземних арбітражних рішень, в тому числі, прийнятих шляхом онлайн-арбітражу..

На даний час не існує «загальноприйнятих правил регулювання арбітражного провадження в режимі онлайн». Такі провадження, безумовно, мають місце, хоча вичерпна статистика щодо електронного арбітражу, схоже, не була опублікована. Очікується, що в онлайн-арбітражі сторони, арбітражний суд, експерти та свідки використовуватимуть електронні пристрої для участі в арбітражному розгляді. Це передбачає використання складних програмно-апаратних пристроїв. Існуючі системи, однак, піддаються критиці на тій підставі, що вони можуть мати справу лише з «дуже обмеженими класами спорів, спрощеним або базовим арбітражним процесом, початком процесу до того, як стануть необхідними змінами, процесом, який використовується одним арбітражним провайдером» (*Julio Cesar Betancourt, Elina Zlatanska, 2013*).

Впровадження онлайн-арбітражу майже не має значущих перешкод, але вимагає вирішення практичних питань ідентифікації сторін електронної комунікації та їх представників, а також розробки систем обміну електронними документами. Останні десятиліття показують, що галузь арбітражу стала основним джерелом інновацій у вирішенні конфліктів. Застосування сучасних інформаційних технологій у проведенні конкретних арбітражних розглядів має безсумнівні переваги, такі як зручність, підвищення якості розгляду та економія витрат.

Однак перехід до онлайн-формату арбітражу може викликати певні проблеми, такі як питання безпеки та припустимості доказів. До того часу, поки уніфіковані правила на міжнародному рівні не будуть визначені, арбітражні установи будуть змушені індивідуально розв'язувати питання, враховуючи конкретні обставини кожного випадку. Наприклад, чи може арбітр у справі між сторонами з Франції та Канади «підписати» арбітражне рішення в електронній формі, і який стандарт електронного підпису слід використовувати.

Для вирішення спорів з використанням онлайн-систем сторонам необхідно надавати докази своїх вимог. Підготовка та представлення доказів вимагає часу і зусиль, що може призвести до уникнення подання непідтверджених позовів.

Можна стверджувати, що електронний арбітраж суттєво знижує транзакційні витрати на вирішення спорів, і це може бути правдою в деяких випадках, але жодних

досліджень на користь цього твердження не було проведено. Загалом можна сказати, що прийняття рішень третьою стороною (арбітражем) завжди потенційно дорожче, ніж спільне прийняття рішень.

З точки зору доцільності онлайн-арбітражу, слід зазначити, що він особливо доречний щодо простих фактів і невеликих за сумою майнових претензій. Отже, онлайн-арбітраж може сподобатися користувачам незначних позовів та арбітражних схем, що складаються лише з документів, але точно не для користувачів «міжнародного арбітражу», де на кону стоять складні питання та великі суми грошей. Це, ймовірно, одна з причин передбачуваної «низької привабливості віртуального арбітражу» в цій сфері. Можливо, електронний арбітраж має розвиватися далі, перш ніж можна буде провести повну оцінку його ефективності, але малоймовірно, що «міжнародний арбітраж», зокрема, коли-небудь відбуватиметься повністю онлайн.

Отже, незважаючи на деякі оптимістичні прогнози щодо потенціалу альтернативного вирішення спорів об'єднатися на рівних умовах з традиційними методами, ще занадто рано прогнозувати, яким може бути майбутнє у таких формах арбітражу. Переваги технологічного прогресу в галузі вирішення спорів, мабуть, переоцінені. АВС – це просто «інший» варіант, і в деяких випадках це може бути навіть найкращим варіантом, але це точно не панацея. Класична система вирішення спорів являє собою складну систему, яку не можна замінити більш швидкими мікропроцесорами і більшими платами пам'яті. Механізми вирішення спорів, як правило, є засобом підтримання суспільного порядку. Ці механізми призначені для вирішення конфліктів і суперечок - на основі верховенства права – і сумнівно, що така функція може повноцінно та ефективно виконуватися в кіберпросторі.

Висновки. Отже, міжнародний досвід свідчить про необхідність реформування національного арбітражу:

- розробка електронних платформ,
- законодавче закріплення цифрових процедур,
- удосконалення цифрових технологій з метою забезпечення інформаційної безпеки учасників розгляду справи в арбітражному процесі.

Цифровізація арбітражу підвищує ефективність, забезпечує захист прав сторін та сприяє зменшенню витрат.

Незважаючи на деякі оптимістичні прогнози щодо потенціалу альтернативного вирішення спорів об'єднатися на рівних умовах з традиційними методами, ще занадто рано прогнозувати, яким може бути майбутнє у таких формах арбітражу. Переваги технологічного прогресу в галузі вирішення спорів, мабуть, переоцінені. АВС – це просто «інший» варіант, і в деяких випадках це може бути навіть найкращим варіантом, але це точно не панацея. Класична система вирішення спорів являє собою складну систему, яку не можна замінити більш швидкими мікропроцесорами і більшими платами пам'яті. Механізми вирішення спорів, як правило, є засобом підтримання суспільного порядку. Ці механізми призначені для вирішення конфліктів і суперечок – на основі верховенства права – і сумнівно, що така функція може повноцінно та ефективно виконуватися в кіберпросторі. Застосування ОВС може надалі вийти за межі онлайн-спорів, що може привчити громадян більш уважно та відповідально ставитися до кожного спору, і таким чином сприяти системному прогресу.

References:

- 2018 DIS Arbitration Rules. URL: <https://surl.li/ijrzok> (дата звернення: 12.03.2025).
- Alejandro E. Almaguer et al., Shaping New Legal Frontiers: Dispute Resolution for the Internet. *Ohio State Journal on Dispute Resolution*. 1998. URL: <https://surl.li/fatzax> (дата звернення: 12.03.2025).
- Scientific Bulletin of Dnipropetrovsk State University of Internal Affairs. 2023. Special Issue № 1
- Avsiyevych A. Prospects of information technology use in international commercial arbitration dispute resolution. *Scientific Bulletin of Dnipropetrovsk State University of Internal Affairs*. 2023. Special Issue № 1. P.114-117. DOI 10.31733/2078-3566-2023-5-114-117.
- Born, Gary B., Anneliese Day, Hafez Virjee. Chapter 7: Empirical Study of Experiences with Remote Hearings: A Survey of Users' Views. *International Arbitration and the COVID-19 Revolution*, edited by Maxi Scherer, Niuscha Bassiri, and Mohamed S. Abdel Wahab. Alphen aan den Rijn: *Kluwer Law International*. 2020, P. 137-150 <https://doi.org/10.54648/joia2021014>
- Chaduteau, O. Panorama des legaltechs. *Enjeux numeriques*. 2018. Vol. 3. P. 77-80. URL: <https://surl.li/ecybfu> (дата звернення: 12.03.2025).
- Chartered Institute of Arbitrators, Costs of International Arbitration Survey. London: Chartered Institute of Arbitrators, 2011, p.2. URL: <https://surl.li/ycwdgr> (дата звернення: 12.03.2025).
- Cohen, S., Morril M. Fordham International Arbitration & Mediation Conference Issue: a Call to Cyberarms: the International Arbitrator's Duty to Avoid Digital Intrusion. *Fordham International Law Journal*. 2016. Vol. 40. P. 981-986. URL: <https://surl.li/ztuvzm> (дата звернення: 10.03.2025).
- Colin Rule. Online Dispute Resolution for Business. San Francisco: Jossey-Bass, 2002. URL: <https://surl.li/cc/puqgun> (дата звернення: 12.03.2025).
- Ethan, Katsh. Bringing Online Dispute Resolution to Virtual Worlds: Creating Processes through Code. *New York Law School Law Review*. 2004. № 49. P.275 URL: <https://surl.li/emucbq> (дата звернення: 10.03.2025).
- Dusseaux, A., Ruggieri H. Doctrine.fr: l'intelligence artificielle au service du droit. *Enjeux numeriques*. 2018. Vol. 3. P. 81-85. URL: <https://surl.li/ssawml> (дата звернення: 12.03.2025).
- E. Casey Lide, ADR and Cyberspace: The Role of Alternative Dispute Resolution in Online Commerce, Intellectual Property and Defamation. *Ohio State Journal on Dispute Resolution*. 1996. № 12. P.719. URL: <https://core.ac.uk/download/pdf/159571987.pdf>. (дата звернення: 12.03.2025).
- Ethan Katsh et al., Online Dispute Resolution: Resolving Conflicts in Cyberspace. San Francisco: Jossey-Bass, 2001, pp.1–240. URL: <https://archive.org/details/onlinedisputeres0000kats>. (дата звернення: 01.03.2025).
- Frank Sander. Iternative Methods of Dispute Resolution: An Overview. *University of Florida Law Review*. 1985. № 37 (1). URL: <https://surl.li/ajbjqu> (дата звернення: 01.03.2025).
- Geneva Ministerial Declaration on global electronic commerce. World Trade Organisation. 1998. URL: <https://surl.li/wtzhpx> (дата звернення: 12.03.2025).
- Guidance Note on Possible Measures Aimed at Mitigating the Effects of the COVID-19 Pandemic, ICC International Chamber of Commerce, 2020. URL: <https://surl.li/yiniad> (дата звернення: 02.03.2025).
- Guidance Note on Remote Dispute Resolution Proceedings, 2020. URL: <https://surl.li/gd/pvcvci> (дата звернення: 12.03.2025).
- Larret-Chahine, L. L'ethique de la justice predictive. *Enjeux numeriques*. 2018. Vol. 3. P. 86-91. URL: <https://surl.li/cc/istsaa> (дата звернення: 12.03.2025).
- Oral hearings in times of COVID-19. URL: <https://surl.li/fnjgui> (дата звернення: 12.03.2025).
- Rules of Arbitration of the International Chamber of Commerce, 2017. URL: <https://surl.li/sinkmg> (дата звернення: 12.03.2025).
- SCC PLATFORM: Guidelines for parties and arbitral tribunals latest revision. May 25, 2020. URL: <https://surl.li/pukarw> (дата звернення: 12.03.2025).
- Scherer Maxi. Remote Hearings in International Arbitration: An Analytical Framework. *Journal of International Arbitration*. 2020. Issue 4, pp. 407-448. URL: <https://surl.li/efzclu> (дата звернення: 12.03.2025).
- Waincymer, J. Procedure and Evidence in International Arbitration. The Hague : Wolters Kluwer, 2012. 1408 p. URL: <https://surl.li/lzaqti> (дата звернення: 02.03.2025).

- Арбітражний регламент ICC (2012). URL: <https://surl.li/kqmgnl> (дата звернення: 12.03.2025).
- Арбітражний регламент Віденського міжнародного арбітражного центру 2021 р. URL: <https://surl.li/dqmusp> (дата звернення: 12.03.2025).
- Бевз Г. М., Петренко І. В. Соціальний конфлікт: Інноваційні комунікативні технології врегулювання: практичний посібник. URL: <https://surl.li/uwgoop> (дата звернення 01.03.2025).
- Варакіна О., Хітрих М. Арбітражна інституція: за якими критеріями обирати? *Юридична газета online*. 2020. № 9 (715). URL: <https://surl.li/qqpnb> (дата звернення: 12.03.2025).
- Доменні спори: різниця між підходами у розгляді акредитованими установами по UDRP та українськими судами. URL: <https://surl.li/blmzgh> (дата звернення 01.02.2025).
- Калаченкова К. О., Сінельник В. І. Технологічні інновації у сфері вирішення спорів: онлайн-підходи. *Правничий часопис Донецького національного університету ім. Василя Стуса*. 2023. № 2. С.75-84. DOI 10.31558/2786-5835.2023.2.9
- Кравцов С. Віртуальний арбітражний розгляд зовнішньоекономічних спорів. *Зовнішня торгівля: економіка, фінанси, право*. 2023. № 4. С.73-87. DOI: [10.31617/3.2023\(129\)07](https://doi.org/10.31617/3.2023(129)07)
- Окінавська хартія глобального інформаційного суспільства: міжнародний документ від 22.07.2000 р. URL: http://zakon2.rada.gov.ua/laws/show/998_163 (дата звернення: 12.03.2025).
- Попов С. Переваги врегулювання спорів онлайн: міжнародний досвід. *Судово-юридична газета*. Грудень, 2019. URL: <https://surl.li/fxcvqq> (дата звернення: 12.03.2025).
- Притика Ю.Д. Онлайн-арбітраж у системі альтернативних способів вирішення спорів: pro et contra. *Проблеми цивільного права і процесу* : тези доп. учасників наук.-практ. конф., присвяч. світлій пам'яті О. А. Пушкіна, Харків, 25 трав. 2018 р. С.58-61. URL: <https://surl.li/wuxify> (дата звернення: 24.03.2025).
- Цірат Г. А. Міжнародний комерційний арбітраж : навч. посіб. / Г.А. Цірат. К.: Алерта, 2019. 410 с. URL: <https://surl.li/xgsbpd> (дата звернення: 24.03.2025).

CHAPTER 3.

INFORMATION BASES OF APPLICATION OPTIONS UNMANNED AERIAL VEHICLES (UAVS) OF THE FPV TYPE AND COUNTERING THEM IN COMBAT CONDITIONS

Oleg BATIUK

Doctor of Legal sciences, Assistant Professor
Professor of the Department of National Security
Lesya Ukrainka Volyn National University (Lutsk, Ukraine)

olegbatiukibrlpnt@gmail.com
<https://orcid.org/0000-0002-2291-4247>

Loenid DANYLIVSKIY

Senior Lecturer of the Department of Intelligence
at the Kyiv Institute of the National Guard of Ukraine,
Major General (Retired),

l.danilevskiy@kr.net
<https://orcid.org/0000-0003-1995-7980>

Andriy PASICHNYK

Lecturer at the Department of Military Communications and Informatization
National Academy of National Guard of Ukraine

pasechnik81@gmail.com
<https://orcid.org/0000-0001-9570-9888>

Annotation. In the provisions of the scientific work, the study conducted by the authors examines the information bases of options for the use of unmanned aerial vehicles (UAVs) of the FPV type and counteraction to them in combat conditions. The authors determine that the use of UAVs of various types on the battlefield has a significant advantage or no alternative at all compared to manned vehicles, namely: the possibility of continuous aerial reconnaissance in the interests of tactical command and control units; the possibility of long-term (24 hours) monitoring of large areas at considerable distances from the control point to obtain real-time operational information. An important characteristic trend of modern combat is the massive application of strikes using ‘barrage’ munitions (‘kamikaze drones’), FPV drones and attack UAVs, which are used to hit targets both at short distances (up to tens of kilometres) and hundreds of kilometres. The systematic use of these types of weapons has largely levelled the relative security at the “front and rear”, demoralised the enemy, and significantly disrupted logistics and control of troops. It is the technological development of FPV drones and related components for their intended use (increased range and flight time, payload weight, increased resistance to enemy EWS, the ability to use in conditions of limited visibility (at night), an increase in the range of ammunition used, the introduction of artificial intelligence for target acquisition, the creation and scaling of specialised training centres for UAV operators) that has led to an increase in possible uses (new tactics) and and expansion of the range of tasks performed with their help. As a conclusion, the authors note

that the constant combat duty of drones in the air has led to decentralisation and reduction of troops on the front line. It is worth noting that the basic tactics of defensive combat, which used to be a platoon, are now being handled by a squad. Where there used to be a 'squad stronghold', there are now three 'holes' of 2 men each. Both sides seek to minimise the movement of combat personnel. One 'armour' can involve up to a dozen UAVs, or 'birds' as they are colloquially known, and 2-3 drones will be involved in the pursuit of a soldier. In the combat zone, reconnaissance drones, bombers and FPV teams are on standby in their respective sectors in shifts, some searching, some striking. Thus, technical development, the use of new tactics and the adoption of FPV drones to the modern battlefield have led to a significant expansion of the range of combat missions they perform. The demand of combat units for trained and experienced FPV drones exceeds the supply on the 'war market'. The innovative development of this type of weapon will undoubtedly entail the search for and implementation of new technical solutions and methods of counteraction (electronic, optical, mechanical, etc.), and will lead to the creation of separate structural units for both their use and counteraction. At the same time, in the near future, certain elements of countermeasures will affect every soldier in combat units. The authors note that the 'competition' in the 'drone-anti-drone' category is just beginning.

Keywords: information, communication, unmanned aerial systems, aircraft, combat operations, countermeasures against UAVs, FPV - drones.

Introduction. The rapid development of scientific and technological progress in the early 2000s led to the possibility of developing and practically using unmanned systems. First Person View, or FPV, is an unmanned aerial vehicle, hereinafter referred to as a UAV, controlled from the first person view, which began to be mass-produced in 2010 due to the development of wireless communication and the improvement of compact cameras. These changes have significantly improved manoeuvrability and control accuracy, opening up new opportunities for FPV drones to be used in professional fields ranging from cinematography and mapping to military operations. Due to the global challenges of active hostilities on the territory of Ukraine since 2014, the use of modern means of destroying the enemy has become necessary to achieve combat objectives with minimal losses of personnel and military equipment. It should be noted that in modern combat conditions, FPV drones play a special role, as they are capable of destroying targets thousands of times more expensive than their own cost. Since 2022, FPV UAVs have been indispensable on the battlefield, as they can easily penetrate dugouts and are capable of destroying various enemy military equipment and enemy personnel (manpower). It is worth noting that the first use of FPV UAVs in the Russian-Ukrainian war was recorded in June 2022 by the Signum 93 unit of the Separate Motorised Brigade of the Armed Forces of Ukraine, hereinafter referred to as the AFU's OMBR. It should be noted that according to official sources, this is the date when the history of the evolution of FPV UAVs begins, which was a response to the constant changes at the front (*FPV drones and their role...*, 2025).

HISTORY OF THE USE OF FPV-TYPE UAVS IN COMBAT.

February 2022 - reconnaissance.

In February 2022, the realisation that cheap Chinese 'wedding' Mavic drones could be adapted to military needs began to spread. So, enemy positions were scouted with civilian copters with simple controls that even an inexperienced operator could understand.

March 2022 - fragmentation grenade drops.

At the beginning of the Russian invasion, Ukrainian drone hobbyists developed FPV

mounts to which they attached small items such as food or medicine. These things were quickly delivered to the trenches. At the same time, the idea of dropping fragmentation grenades such as VOG-17/VOG-25 was spread to the frontline and picked up by various units.

Drone operators countered the Russians in small groups. Some were flying FPVs with suspended grenades at the target, while others were adjusting the attack from reconnaissance drones. During such attacks, one operator could use up a box of fragmentation grenades per day.

Later, the drop systems were modified by printing tail stabilisers for the shells on 3D printers so that the drops would not be blown away by wind gusts. And this made it possible to hit targets more accurately from a height.

April 2022 - kamikaze drones.

The SIGNUM unit was one of the first to use kamikaze drones at the front. This is what FPV operator Serhii Z. with the call sign Schweiger tells about. It was the spring of 2022. That's when volunteers handed over a sports drone to their volunteer unit. The military installed a more powerful video transmitter, bought goggles and attached a detonator.

According to operator Schweiger, the first drone almost missed its target because the battery failed. But the problem was fixed and a few months later, they began to hit the enemy with their kamikaze drones. This innovation was extended to other units.

The arrival of FPV strike drones at the frontline dramatically changed the nature of the war. Expensive military equipment was being destroyed by cheap drones.

July 2022 - heavy FPV bombers with night vision.

In the summer of 2022, the Russians started talking about Baba Yaga. These were heavy Vampire FPV drones with thermal imagers capable of carrying up to 20 kg of explosives, which were dropped on their positions.

The eight-engine R18 night drone can carry several hand-held rocket-propelled grenades (RKGs), which are used to bomb tanks, armoured vehicles and defences. If the first round fails to hit the target, the next round completes the job after the operator adjusts the trajectory.

March 2023 - remote mining.

In the spring of 2023, the Ministry of Defence allowed FPVs to operate at the front, carrying modified anti-tank mines and laying them on the ground. These drones can travel at speeds of up to 120 km/h.

The mines dropped by the drones have an electric detonator that is activated after contact with the ground. This detonator operates on a battery charge for up to two weeks. It receives signals from a built-in magnetometer, gyroscope and accelerometer. This system activates the explosion when the mine is moved or if it is hit by heavy machinery.

August 2023 - automatic targeting.

In the summer of 2023, Ukrainian specialists developed an FPV with auto-targeting. The operator only marks the object, and then the drone's on-board computer takes over and flies independently on a course towards the military equipment.

If an enemy EWS jams the communication, the drone still attacks the designated target. According to the developers, such FPVs can catch up with moving objects.

September 2023 - drones with machine vision.

In September 2023, the Defence Forces received another set of artificial intelligence drones. It includes a reconnaissance drone with advanced optics and kamikaze drones.

The reconnaissance drone can detect even camouflaged enemy vehicles, record their coordinates and transmit this data to the command post. He can distinguish a tank from artillery, a military vehicle from a civilian one, etc. Then, kamikaze drones are sent to the spot to destroy the target.

Such FPVs can distinguish between more than 60 types of military targets. The drones are trained to detect new, unknown objects. The collected data is fed into the Delta intelligence system, which creates a map of the battlefield. In this way, FPVs do the work that would take hundreds of hours for a human to do.

October 2023 - aerial detonation of munitions.

The Ukrainian forces have begun to use FPVs to detonate warheads in the air. These drones are equipped with high-explosive fragmentation shells, and the drone operator activates the explosion at the right time.

The Defence Forces use these drones to destroy enemy infantry hiding behind obstacles. The fragments are scattered over a large area and hit enemy manpower in the area of operation.

November 2023 - increase in the flight range of FPV drones to 25 km.

Small FPV drones hit targets at a distance of 3-4 km. They cannot fly further due to limited radio communication. When a drone flies over uneven terrain or over the horizon, the signal is lost.

In the autumn of 2023, Ukrainian units extended the flight range of their kamikaze drones to 25 km. Signal repeaters were installed on heavy FPV drones. Drones with such transmitters follow short-range drones and increase their communication coverage. In turn, they attack equipment hidden away from the contact line.

February 2024 - FPV with EW protection.

SkyLab UA engineers have created an FPV drone with enhanced protection against electronic warfare system (EWS). These drones have duplicate communication modems. If the signal is jammed, the drone operator switches to another modem.

When the enemy suppresses the first stage of protection, the GPS receiver is switched on with filters that automatically pick up the strongest signals from the satellites. In this way, FPV can withstand several enemy electronic warfare jamming.

In case of jamming of both communication systems, the drone operator is guided by the camera image. That is, if the signal from the modems and GPS receiver disappears, the drone returns to the base.

June 2024 - downing of reconnaissance drones.

In the summer of 2024, the web was flooded with videos of Ukrainian FPVs shooting down Russian Orlan, Supercam and ZALA drones. These enemy reconnaissance drones fly behind the front line at a distance of more than 70 km and track our troops, equipment, air defence systems and aircraft. Subsequently, they use kamikaze drones or ballistic missiles to target the objects they find.

To shoot down reconnaissance drones for the Defence Forces, Ukraine has developed FPVs that can rise to an altitude of up to a kilometre and fly at a speed of about 100 km/h. The operator detonates the drone's warhead as it approaches an enemy UAV.

Such FPVs make it cheaper to destroy Russian drones and also save scarce air defence missiles, hereafter referred to as air defence. After all, a single shot at a reconnaissance drone from a Western-style anti-aircraft gun can cost up to half a million dollars.

July 2024 - 'mother ship' drone.

The Wild Hornets community has created the largest FPV drones, the Queen of Hornets. These drones act like kamikazes, dropping projectiles on targets and carrying loads of up to 9.5kg.

The most interesting thing is that such a drone can be a 'mother ship' for other short-range FPVs and carry them over long distances. Kamikaze drones can be dropped into remote Russian positions without using up their battery power.

September 2024 - flying grenade launchers.

The Bulava Unmanned Systems Unit tested an FPV drone with a Bullspike-AP hand-held grenade launcher.

Such copters attack targets from a distance of over 5 km. But they are primarily used in urban battles, when it is necessary to quickly fly at the enemy and hit him with a precision strike. Another option is to destroy damaged equipment that the Russians can still take from the battlefield for repair.

The grenade launcher drones are reusable. They are returned to the base for reloading. And thanks to this, kamikaze drones are less consumed. Disposable FPVs do not always destroy Russian equipment on the first hit. Therefore, operators fly to the target again and again.

'We can't provide any other details about the grenade launcher drones yet, except to say that we will continue to work on it together with the Bulava unit to reach mass production and help our military,' say the developers from Wild Hornets..

September 2024 - drones with automatic weapons.

For the first time in history, the Defence Forces used an FPV drone with an assault rifle to fire on Russian infantry.

In November 2024, soldiers of the Bulava unit repelled an assault by the invaders near Velyka Novosilka in Donetsk Oblast. A column of Russians was destroyed by kamikaze drones, and the Queen of Hornets with an assault rifle attached to it was sent to clear the infantry in the position. During the firefight, this FPV took several bullets from the Russians, but continued the attack. This was reported by the Wild Hornets community, which released a video of their drones.

September 2024 - 'dragon drones'.

In September 2024, Ukrainian drones began burning Russians in their landings with thermite. This mixture of aluminium and iron oxide burns at a temperature of around 2200 degrees. It destroys fortifications, burns through steel or melts the aluminium body of equipment.

One small FPV drone carries up to 1 kg of thermite, and the largest models carry up to 8-9 kg. The termite burns in a continuous strip. It is extremely difficult to extinguish such flames. Therefore, after it is dropped, the infantry flees from the positions and cannot return to their shelters.

December 2024 - drones on fibre optics.

Fibre-optic drones are probably the most popular innovation on the contact line. The Russians are ahead of us in using these FPVs.

Such drones are fitted with spools of wire that unwind as they move towards the target. A stable signal is transmitted through the wire. Therefore, the drone does not respond to communication jammers. The operator receives a clear picture from the digital camera.

The drone flies low, making it difficult to spot.

In December 2024, the Birds of Magyars regiment of attack drones announced the creation of their own fibre-optic FPV drones. According to the regiment's commander, Robert B., this development was submitted to the Ministry of Defence of Ukraine for codification.

December 2024 - FPV drones with shotguns.

In December 2024, the Foundation for Assistance to the Defenders of Ukraine showed a video of a drone with a shotgun shooting down a Russian FPV. In another recording in January 2025, such a drone is seen destroying at least 20 enemy drones.

January 2025 - fibre-optic enemy drone detectors.

This is an experimental method. The Magyar Birds have installed stations that detect the approach of Russian drones using fibre optics.

'Such mobile radars 'see' enemy drones at a distance of 3-4 km. An FPV interceptor flies to the spot and blows it up with a controlled explosion in the air,' says unit commander Robert B. (call sign "Magyar")..

February 2025 - downing of the Shahed by FPV drones.

Ukrainian firing groups are shooting down Shaheds using FPV drones. This was reported by the commander of the Unmanned Systems Forces, Vadym S.

'Mobile groups launch multi-rotor FPVs with a powerful charge of explosives. The drone follows the Russian UAV, and its position in the air is monitored by radar. The FPV enters the Shahed from above and hits it (*Evolution of FPV Drones*, 2025).

THE ROLE OF FPV-TYPE UAVS IN COMBAT OPERATIONS.

An analysis of the use of FPV drones by both the enemy and the Armed Forces of Ukraine shows a significant increase in their role in combat operations as an effective means of combat destruction. Their widespread use by both sides significantly affected the course of hostilities and led to changes in the tactics of employment of combined arms units. Due to their low weight, they are capable of carrying a payload to the target (several times their own weight) at a speed of 10 km/h over a distance of 10 km or more.

In terms of percentage, FPV-TYPE strike UAVs account for a significant share (up to 70 per cent) in performing tasks of combat destruction of the enemy (manpower, weapons and military equipment, hereinafter referred to as WME, in tactical depth). It is also characteristic that these indicators are absolutely symmetrical (inherent in both sides of the armed conflict).

It is worth noting that the use of UAVs of various types on the battlefield has a significant advantage or no alternatives at all compared to manned vehicles, namely:

a) the possibility of continuous aerial reconnaissance in the interests of tactical command and control units;

b) the possibility of long-term (24 hours) monitoring of large areas at considerable distances from the control point to obtain real-time operational information.

Another distinctive trend was the massive use of 'barrage' munitions ('kamikaze drones'), FPV drones and strike UAVs, which are used to hit targets both at short distances (up to tens of kilometres) and hundreds of kilometres away. The systematic use of these types of weapons has largely levelled the relative security at the 'front and rear', demoralised the enemy, and significantly disrupted logistics and control of troops.

The technological development of FPV drones and related components for their

intended use (increase in range and flight time, payload weight, increased resistance to enemy EWS, ability to use in low visibility conditions (at night), increase in the range of ammunition used, implementation of artificial intelligence for target acquisition, creation and scaling of specialised training centres for UAV operators) has led to an increase in possible uses (new tactics) and expansion of the range of tasks performed with their help.

It is worth noting that it is the performance of fire support tasks by UAV units that has become a new form of fire support. The tactics of integrated firepower use assumes that strike UAVs (together with more traditional means) have a comprehensive effect on the enemy.

The effective massive use of relatively cheap attack UAVs has created atypical problems for the enemy that previously did not significantly affect its combat effectiveness: damage to weapons and military equipment while in motion, remote mining of rearward movement routes, high-precision destruction of surveillance and reconnaissance equipment, etc.

In terms of the use of strike UAVs, certain peculiarities should be noted due to their design, tactical and technical characteristics, and operating rules:

a) fire damage to moving targets.

FPV-type strike UAVs have opened up a unique ability to destroy moving enemy targets at a distance of up to 20 km. Most often, moving targets are engaged to disrupt enemy logistics and are a rapid response to changing combat conditions in tactical depth. Prior to the arrival of FPV drones in the armed forces, high-precision engagement of moving targets was only possible with anti-tank missile systems that required line-of-sight, with the maximum effective range of ATGMs limited to 5 km;

b) counter-battery warfare.

Along with the 'classical' means of counter-battery warfare, such as long-range cannon artillery and MLRS, including HIMARS/MLRS systems, strike UAVs with a cluster warhead are increasingly being used. The choice of the method of destruction will depend on the time of day, the operational and tactical situation, and the technical characteristics of the means of destruction.

FPV drones are mainly used to defeat the enemy during the day.

Multi-rotor UAVs equipped with appropriate equipment capable of hitting targets at a distance of up to 20 km from the take-off point are used to defeat them at night. Strikes are carried out deep into the defence to destroy enemy artillery assets at firing positions or in areas of concentration. Reusable multi-rotor UAVs are also used to engage enemy artillery systems located at a distance of 4-5 km from the contact line (hereinafter - LoC), mostly trailed artillery. The average statistical combat radius of such UAVs is 8 km and strongly depends on the EWS in the area of the mission;

c) destruction of surveillance devices.

FPV drones have been successfully used to engage small-sized targets, such as the Murom-M/P surveillance system or the electronic intelligence and electronic warfare system, hereinafter referred to as EIS/EWS, Strizh-3. Most often, these types of targets are inconspicuous and have an open silhouette. This does not prevent strike UAV units from neutralising this type of target quite effectively. FPV drones allow them to engage such targets with greater accuracy and less consumption than artillery;

d) fire support for the actions of combined arms units.

To perform the task of fire support of offensive (assault) or defensive combined arms units, the entire range of available strike UAVs is used and is usually carried out in two stages (fire training and support of combined arms units);

e) performing tasks as a standby firepower.

Preventing the advance (stopping) of the advancing enemy is achieved through the fire damage of enemy convoys (tanks, infantry fighting vehicles (IFVs), armoured personnel carriers (APCs)) by strike UAVs, disrupting their combat order and creating favourable conditions for destruction (the target is immobilised).

The main advantages of FPV drones over multi-rotor UAVs are as follows:

- a) first-person view control of the drone;
- b) instant feedback and maximum control over the drone;
- c) high speed (up to 120 km/h) and manoeuvrability;
- d) resistance to electronic warfare (due to the modularity of the device, which allows for rapid configuration and settings);
- e) the ability to change the drone design for a specific task;
- c) low cost of the product.

The weaknesses of FPV drones, in comparison with multi-rotor UAVs, include:

- a) the average flight duration of 7-10 minutes;
- b) flight range (without a repeater) up to 10 km;
- c) the need of selection and qualitative training of a pilot, which requires time (at least one month).

The general layout of the FPV drone and its main components are shown in Figure 1.



Figure 1. General layout of the FPV drone.

Strike UAV crews perform combat missions as a regular firepower. At the same time, the most trained and experienced crews perform missions against detected moving targets. After the target is immobilised, the experienced crew redirects to another task, while the less experienced crew continues to fire at the immobilised target with high explosive munitions

until it is guaranteed to be destroyed;

f) performing tasks of complex counteraction to enemy FPV drones.

The experience of using FPV drones by our units allows us to use the acquired knowledge and skills to counteract the enemy's symmetrical actions;

f) performing a combat mission by a swarm of UAVs under the control of an artificial intelligence system.

This method of using UAVs is currently more of a research or test method. Its practical implementation from a technical point of view looks rather complicated, but promising.

The analysis demonstrated the prospects of strike UAVs in the broad sense of the term "firepower". The low cost of hitting a target, enhanced operator safety, range and availability of mass production are the competitive features of the dominant weapon of the near future. There is reason to believe that strike drones could become a critical capability for the Ukraine AF. At the same time, the enemy is also actively developing the use of UAVs, which prompts us to develop means of countering and defending against them.

Informational bases of fpv-type uavs applications methods.

The first method - the classic one - is the use of FPV-Type UAVs.

The most common way to use FPV drones is to search for and detect a target using a reconnaissance UAV and transmit data on the target's location to the FPV drone operator in order to destroy it. Correction (targeting, target illumination) and video recording of the target's destruction is carried out by the reconnaissance UAV operator (Figure 3).



Figure 2 - general structure of an FPV drone.

An FPV drone can fly due to the main components that are properly selected for a specific task.

The main elements of an FPV drone are:

1) frame - the main framework on which all other components are mounted. Its dimensions are measured by the diagonal between two opposing motors;

2) motors (differ in power and can reach high flight speeds);

3) propellers (the size of the propellers that can be installed determines certain characteristics of the frame);

4) flight controller - provides stabilisation and control;

5) FPV camera - has a high resolution and allows you to adjust the viewing angle;
 6) video transmitter - transmits analogue or digital video signals at different distances;
 7) receiver - works with a certain list of protocols and allows receiving a video signal from the drone;

8) engine speed regulator.

A typical FPV drone used by parties of armed conflict has the following characteristics:

- a) drone size - 7 in;
- b) payload - up to 1.5 kg;
- c) maximum speed (with load) - up to 120 km/h;
- d) flight time with payload - 15 minutes;
- e) flight range with payload (without repeater) - 10-12 km;
- f) preparation time for combat use - 2 minutes.

A typical FPV-TYPE UAV crew consists of a senior crew calculator, an FPV drone operator, an ammunition specialist and a reconnaissance drone operator (Figure 3). The effective work of the FPV-TYPE UAV team is ensured by the reconnaissance UAV operator, who searches for the target, corrects the FPV drone pilot's aiming at the target and controls its destruction.

In addition, to pilot an FPV drone, special goggles (monitor) and a remote control (Figure 1), as well as a charger, are required. FPV goggles are designed to provide a first-person view for a high immersion effect and greater control, especially at high speeds. The remote control is the main component that provides communication between the pilot and the drone and allows the control of the device using joysticks and other buttons.

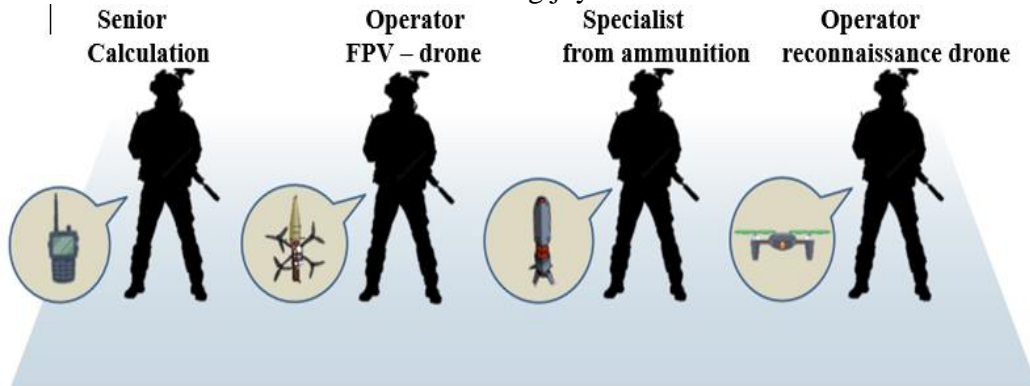


Figure 3. Typical UAVs type calculation FPV

The second method is Free Hunt (FPV drone strike at previously identified targets).

The essence of this method is that the FPV operator flies independently from the take-off point to the area of the previously identified target, conducting and searching for the target on the ground and conducting a strike. This method of use does not require in-flight correction (targeting) and recording of the target's defeat by the reconnaissance UAV (Figure 4).

Figure 4 shows the method of using FPV drones - free hunting.

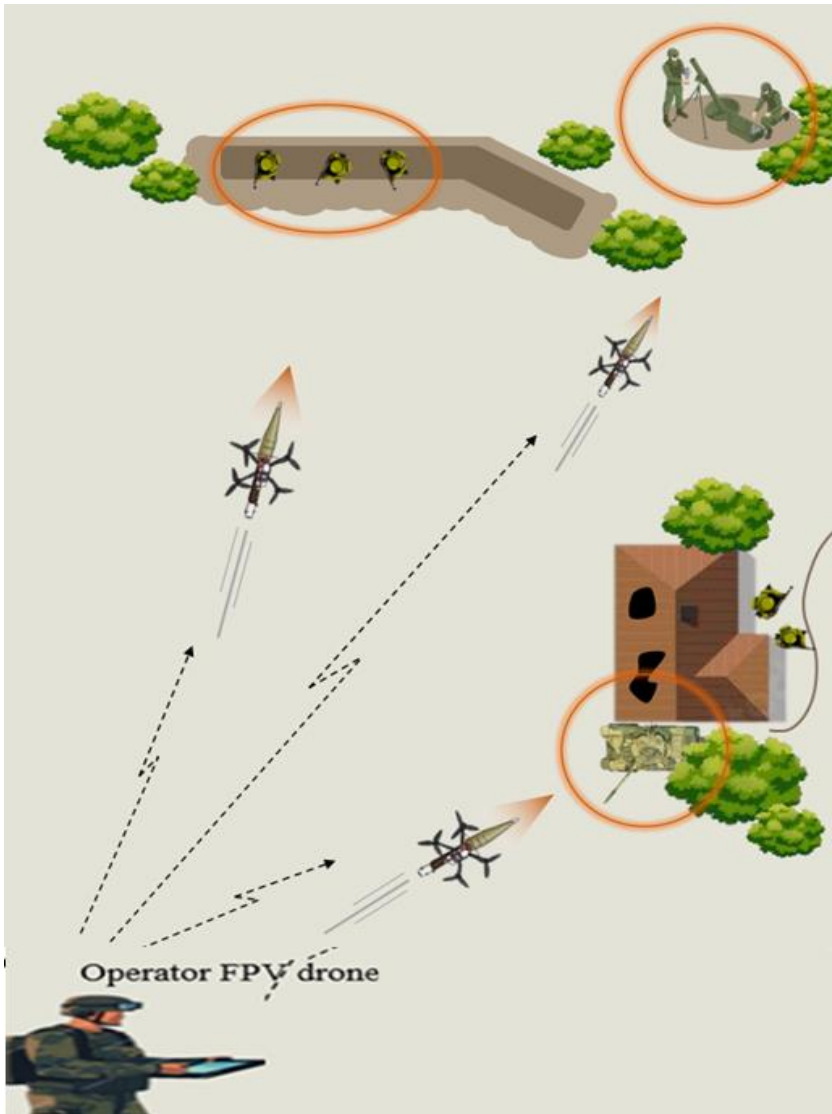


Figure 4. The method of using FPV drones is free hunting.

The third method - FPV drone swarm (FPV drones strike at selected targets).

This method of using FPV drones involves detecting targets (objects of destruction) with the help of a reconnaissance UAV and massively attacking them with disposable strike drones to destroy them. Typically, the total number of FPV drones that can be used simultaneously is 5-12. Reconnaissance drones record the results of the fire damage to identified targets.

This tactical technique involves landing an FPV drone near the area of an ambush, then conducting reconnaissance (surveillance) and suddenly striking the target after it is detected.

This method of using FPV drones is based on taking up a hidden waiting position in advance near high-traffic routes, intersections, bridges, places where equipment and personnel are concentrated, etc., followed by a sudden strike on the target that has been

identified. When used in conjunction with a reconnaissance UAV (UAV with a repeater), the depth of the FPV drone application can be more than 5 km and the time spent in the waiting area can be up to 6 hours (provided that only the control channel receiver is turned on). At night, it is possible to conduct strikes based on the positioning lights (headlights) of moving vehicles, or to use FPV drones with a thermal imaging camera (Figure 5).

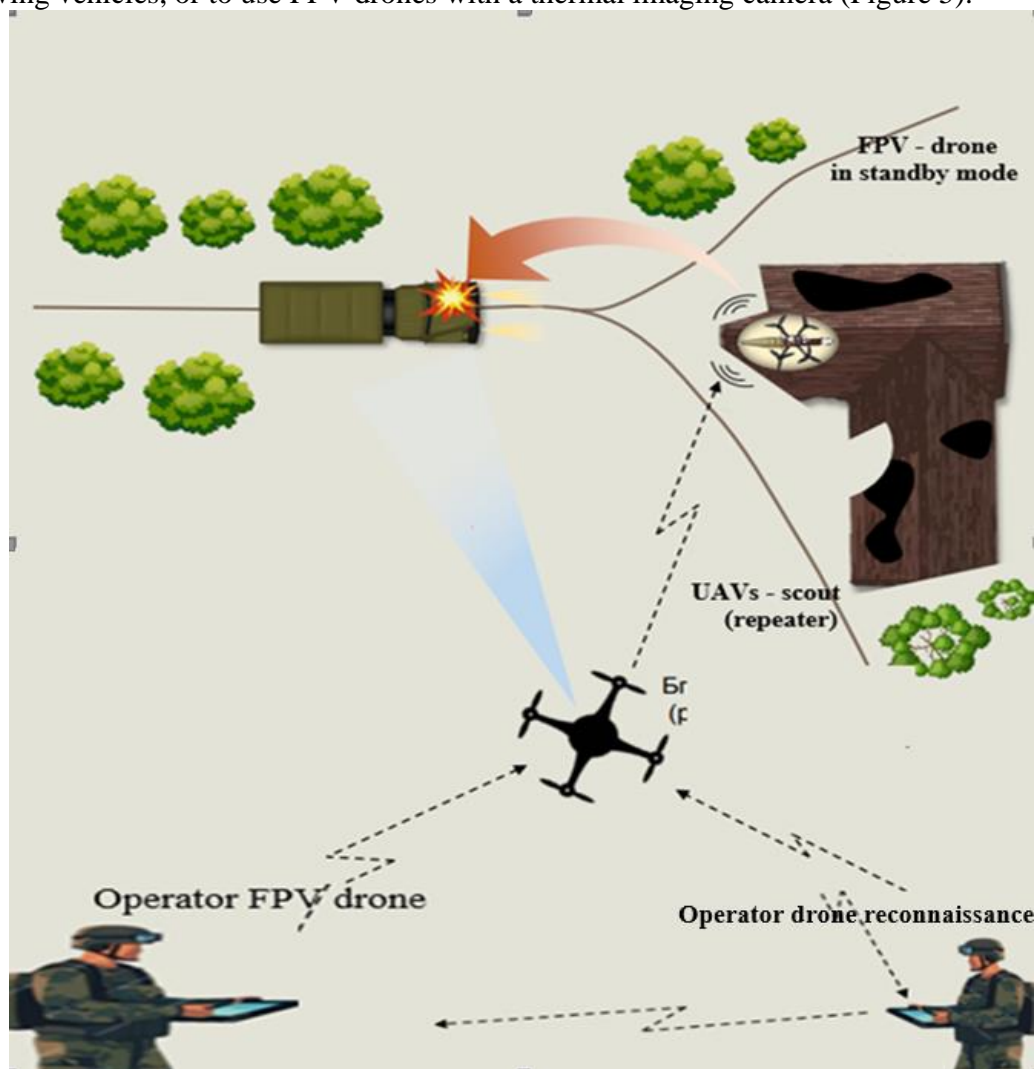


Figure 5. Conducting a fire ambush using an FPV drone.

Fourth method - Combined attack.

This method consists in solving the joint task of FPV drones and reusable strike UAVs (UAVs with drops) to deliver a comprehensive fire attack on identified targets. After the destruction (damage) of an armoured vehicle (object) by an FPV drone strike, a reusable strike UAV drops ammunition on personnel during their evacuation.

Another variant of a combined strike may be to inflict fire damage on personnel (vehicles) by dropping munitions to immobilise them, and then using FPV drones to guarantee their destruction (Figure 6).

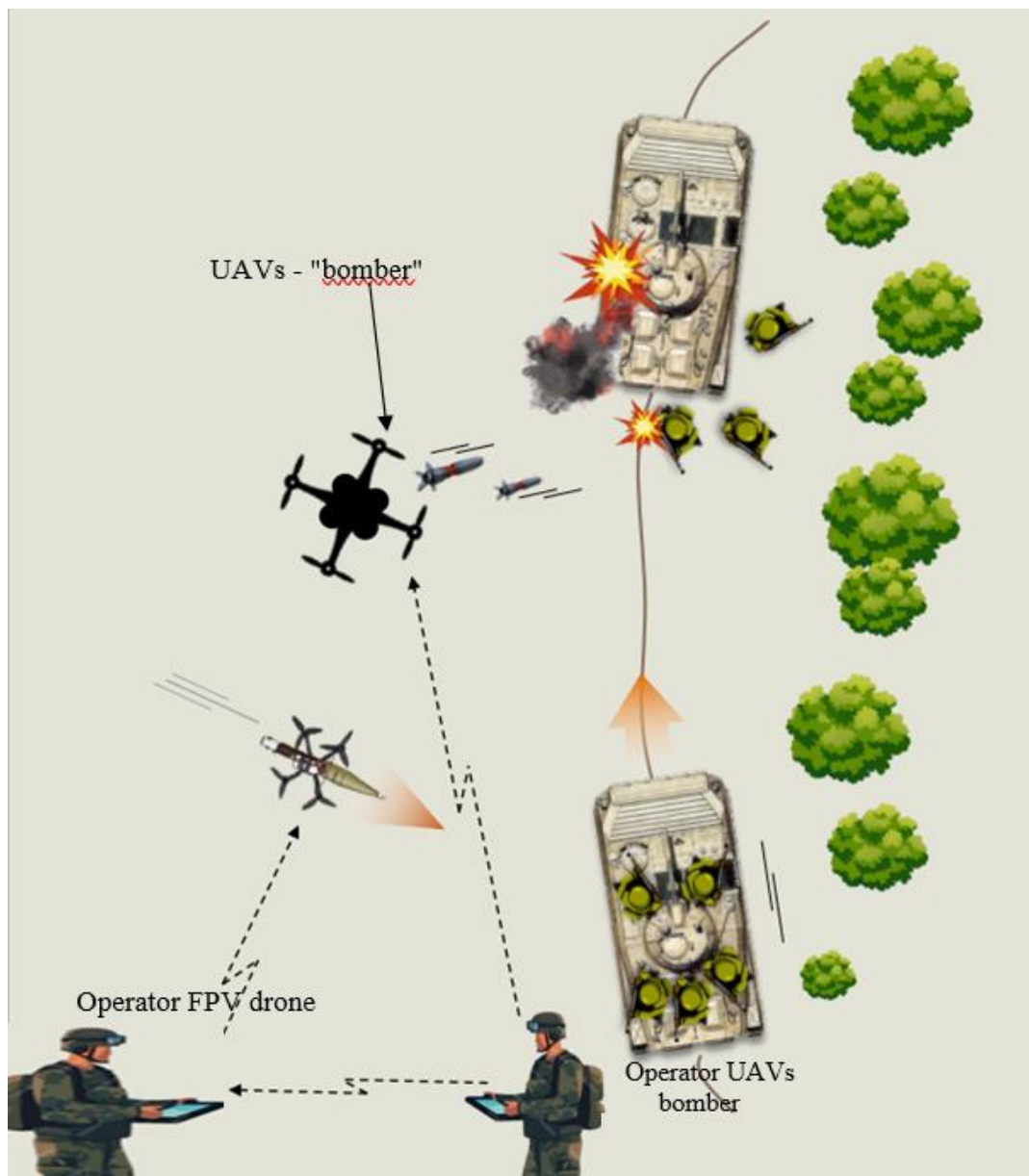


Figure 6. Delivering a combined strike using UAVs.

Fifth method - Double strike

Double strike (the use of two or more FPV drones with different types of warheads to make a passage in a shelter and further destroy enemy personnel).

In order to destroy enemy manpower hiding in protected shelters, several FPV drones are used sequentially: the first one with an explosive warhead to penetrate an obstacle, the second one, usually with a thermobaric or fragmentation warhead, to inflict fire damage on personnel in the interior of the building (Figure 7);

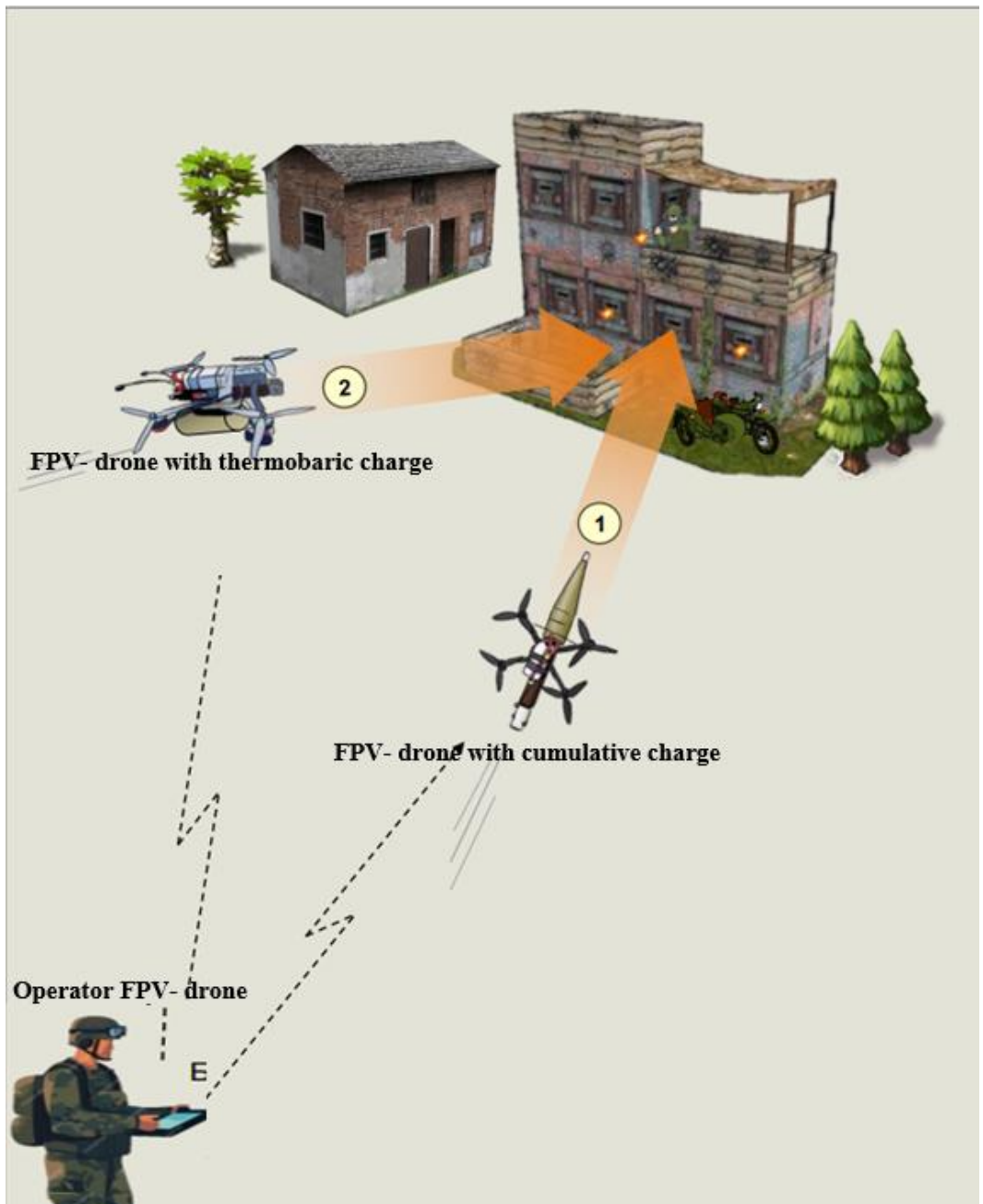


Figure 7. Sequential use of multiple FPV drones with different types of warheads.

Sixth method - Using an FPV drone as a decoy

Given the combat experience of using FPV drones, there are several options for using them as decoys (Figure 8):

a) landing of the drone and sounding a sound signal - when the drone is approached (captured) by enemy personnel, the FPV operator performs a radio-controlled detonation via a reconnaissance UAV (repeater).

b) when its position changes (due to a "Jonik" device), a self-detonation is initiated

(in addition, it is possible to install a magnetic target sensor that reacts to metal);

c) the use of a charge (20-50 g) in the drone's construction, which is activated during its dismantling;

d) a built-in GPS tracker; tracking it will result in fire damage to the location from which the signal is coming;

e) treatment of the drone's body with potent toxic substances of skin-infiltrating effect (this option of using an FPV drone is used by the enemy).

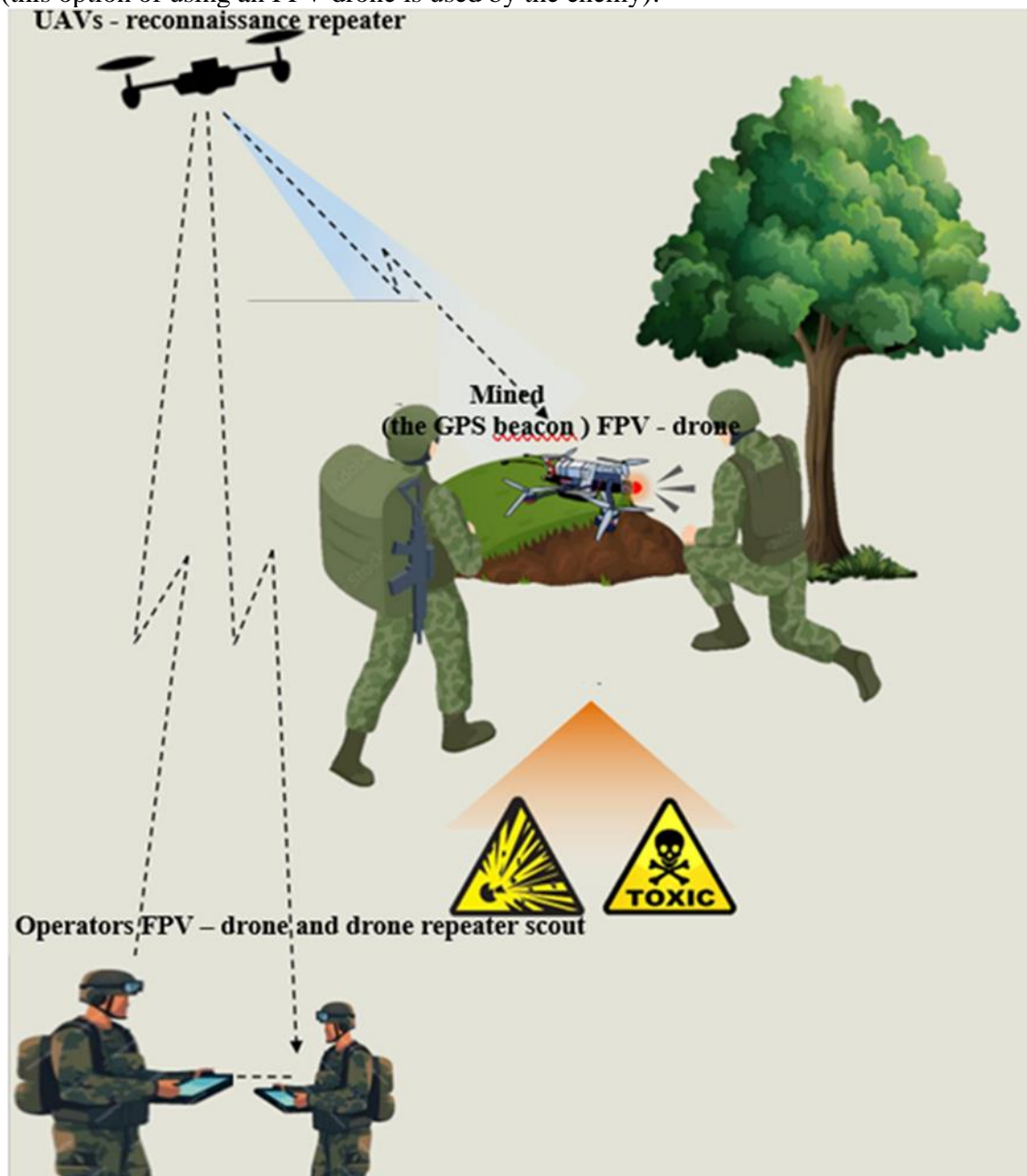


Figure 8 - Using an FPV drone as a decoy.

Seventh method - Using UAVs to remotely mine designated areas.

This method is used to remotely mine designated areas of terrain with UAVs using anti-personnel anti-tank mines and improvised explosive devices. Mines are usually placed on enemy personnel rotation routes, evacuation routes, or near positions (objects) to destroy enemy manpower and equipment (Figure 9).

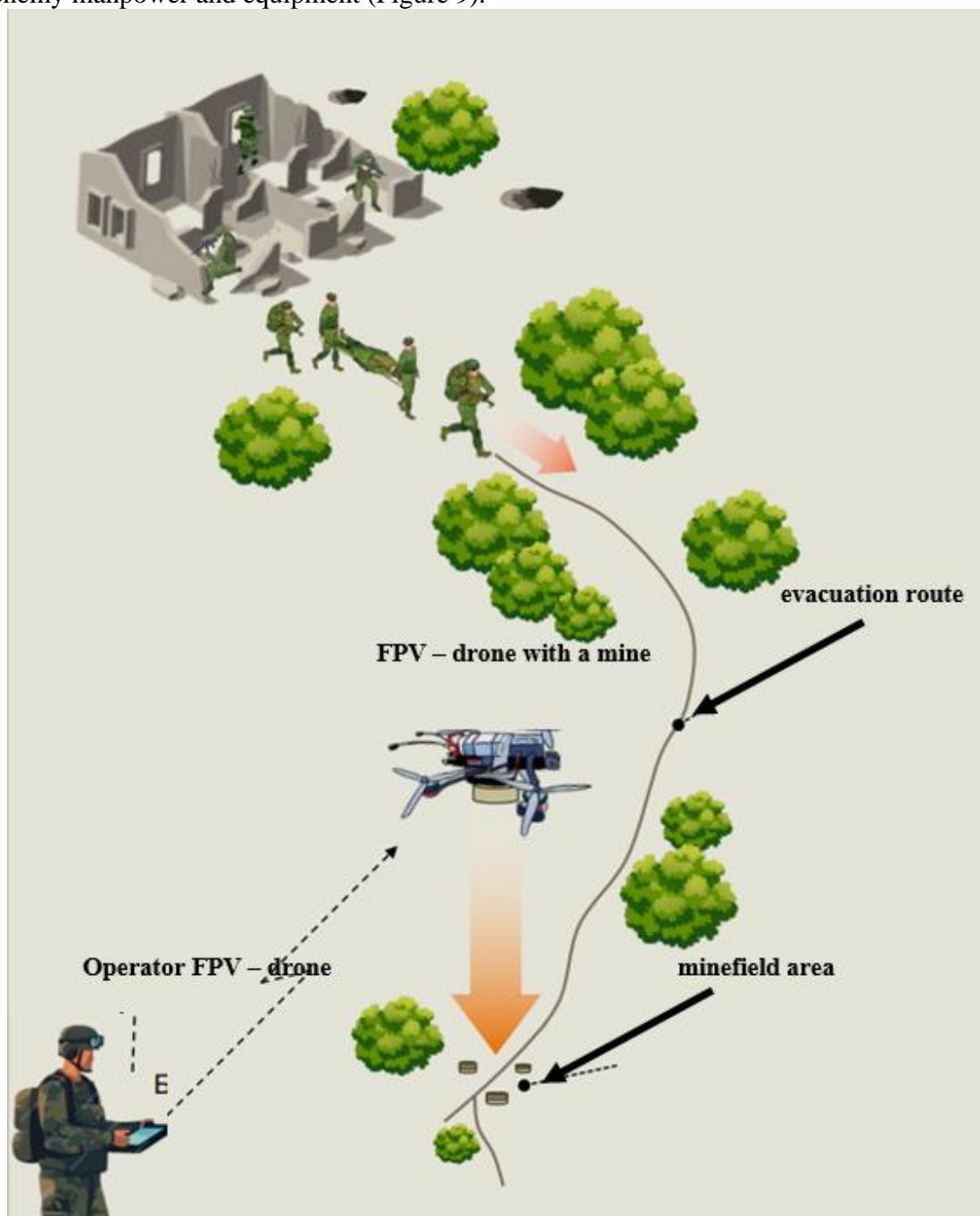


Figure 9. Remote mining of terrain areas with FPV – drone

Eighth method - Using UAVs for demining tasks.

Demining of an area of terrain, usually movement routes, is carried out by dropping ammunition from a UAV or by placing a charge on openly laid and unmasked mines (Figure 10).

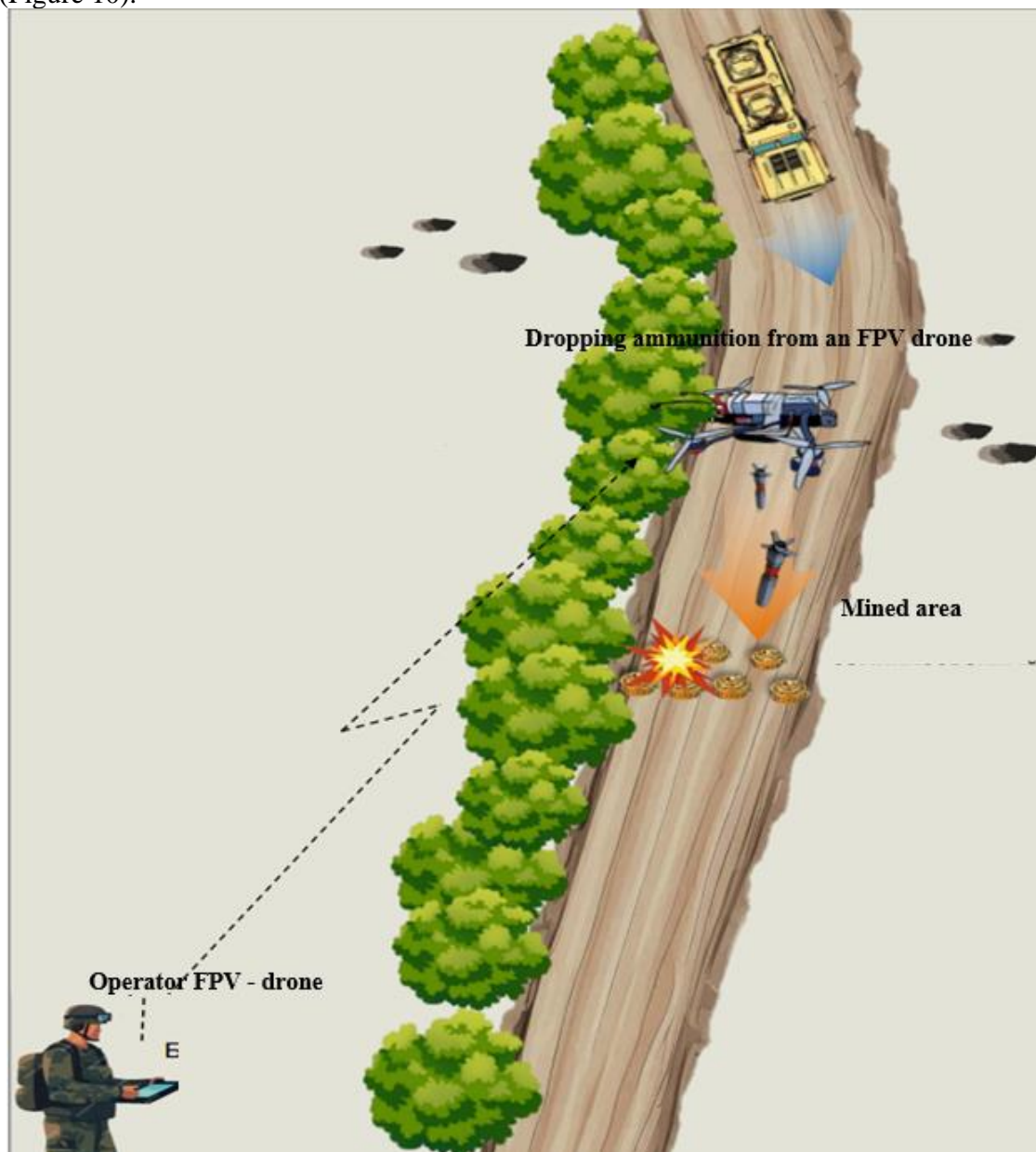


Figure 10. Use of UAVs to perform demining tasks.

The ninth method - the use of FPV drones as attack UAVs.

The tactical technique consists in dropping ammunition from an FPV drone to destroy personnel in open terrain or in a poorly protected shelter ('hole'). The reconnaissance UAV aims the FPV at the target. Cases of the use of ammunition with poisonous substances have been recorded. In addition, this method is often used to drop payloads to their troops (Figure 11).



Figure 11. Using FPV drones as attack UAVs.

The tenth way - the use of FPV drones as incendiary mixture sprayers over enemy positions.

This tactical technique is used to set fire to and disable personnel, equipment, openly located ammunition and property using an FPV equipped with a thermite. Charge (based on a 120 mm artillery incendiary munition). The spray height of the incendiary mixture is 20-50 m. Burning time - up to 2 minutes, temperature over 2300 degrees (Figure 12).

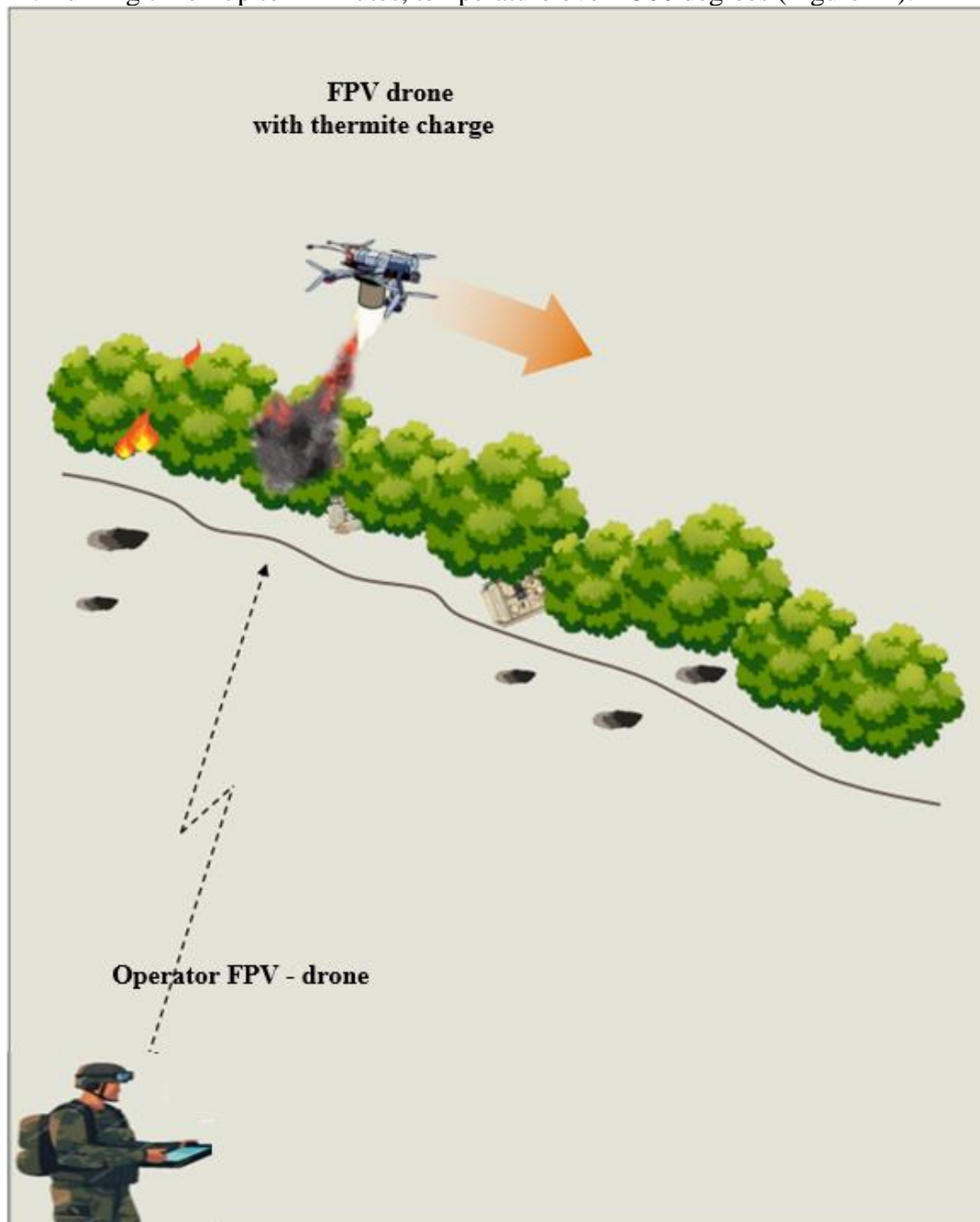


Figure 12. Using an FPV drone as an incendiary sprayer.

The eleventh method - the use of an FPV drone as an interceptor of enemy air targets.

This method is used to combat reconnaissance UAVs of aircraft type and strike UAVs (Lancet barrage munition) using FPV drones. When UAV radio equipment is detected (operating altitude - up to 3 km, speed - up to 110 km/h), FPV drones are launched to intercept and destroy them. The enemy UAV is defeated by detonating a fragmentation charge on approach or by ramming. Targeting is carried out by the operator of the radar station (hereinafter referred to as the radar) (Figure 13).

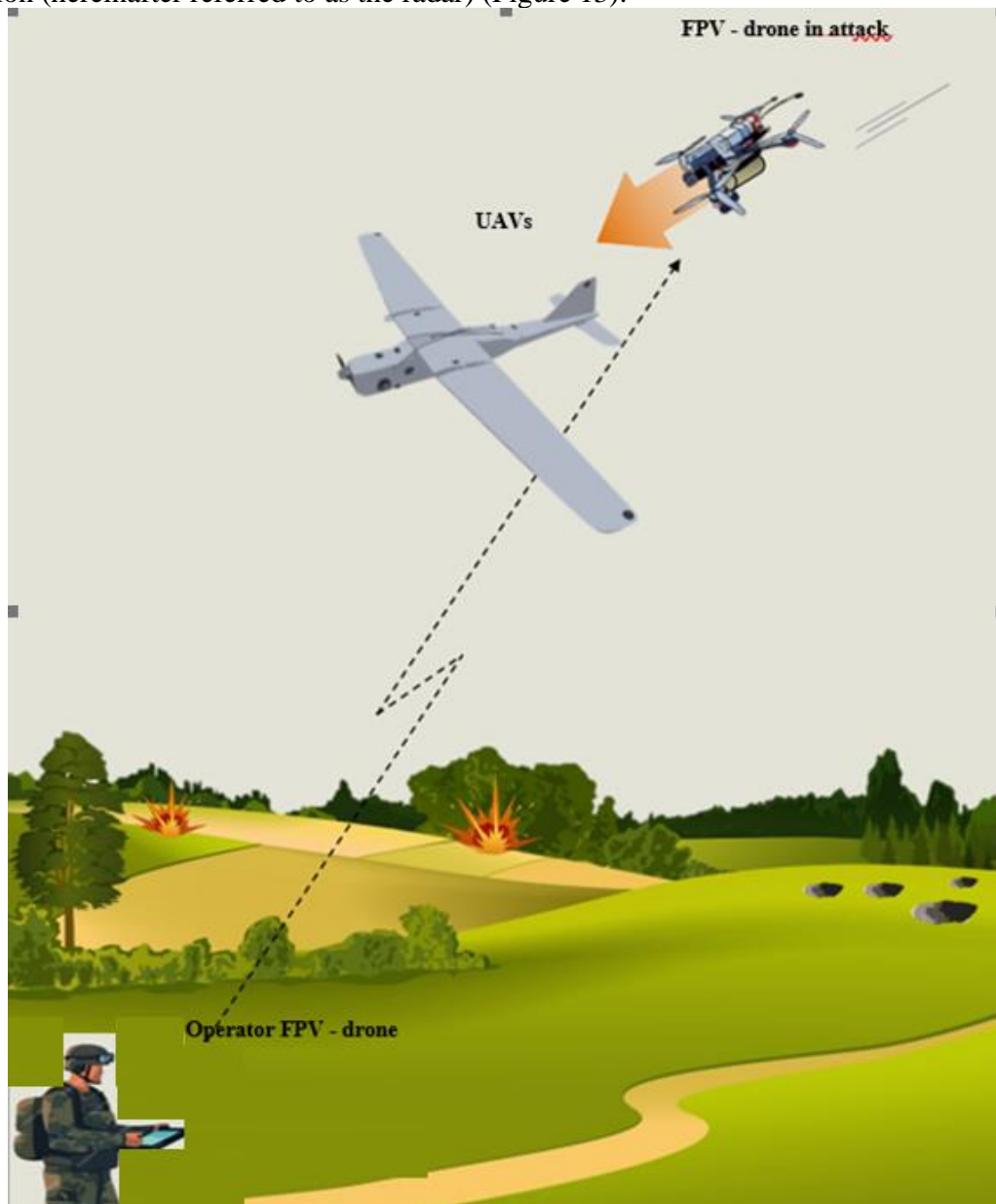


Figure 13. Using an FPV drone as an interceptor of enemy air targets

The twelfth method - the remote use of FPV drones to destroy important enemy targets.

The essence of this method is as follows: covert installation of FPV drones by a sabotage and reconnaissance group (hereinafter referred to as SRG) near objects in the enemy's rear - remote activation of them using pre-loaded coordinates.

This method of using FPV drones is used by SRGs to destroy (disable) enemy military equipment and facilities. After the SRG covertly installs 'kamikaze' drones (4-6 pcs.) near the object at a distance of up to 2-3 km and switches to the 'standby' mode, the UAVs are remotely activated via a GSM network signal to strike targets in accordance with pre-loaded coordinates (Figure 14).

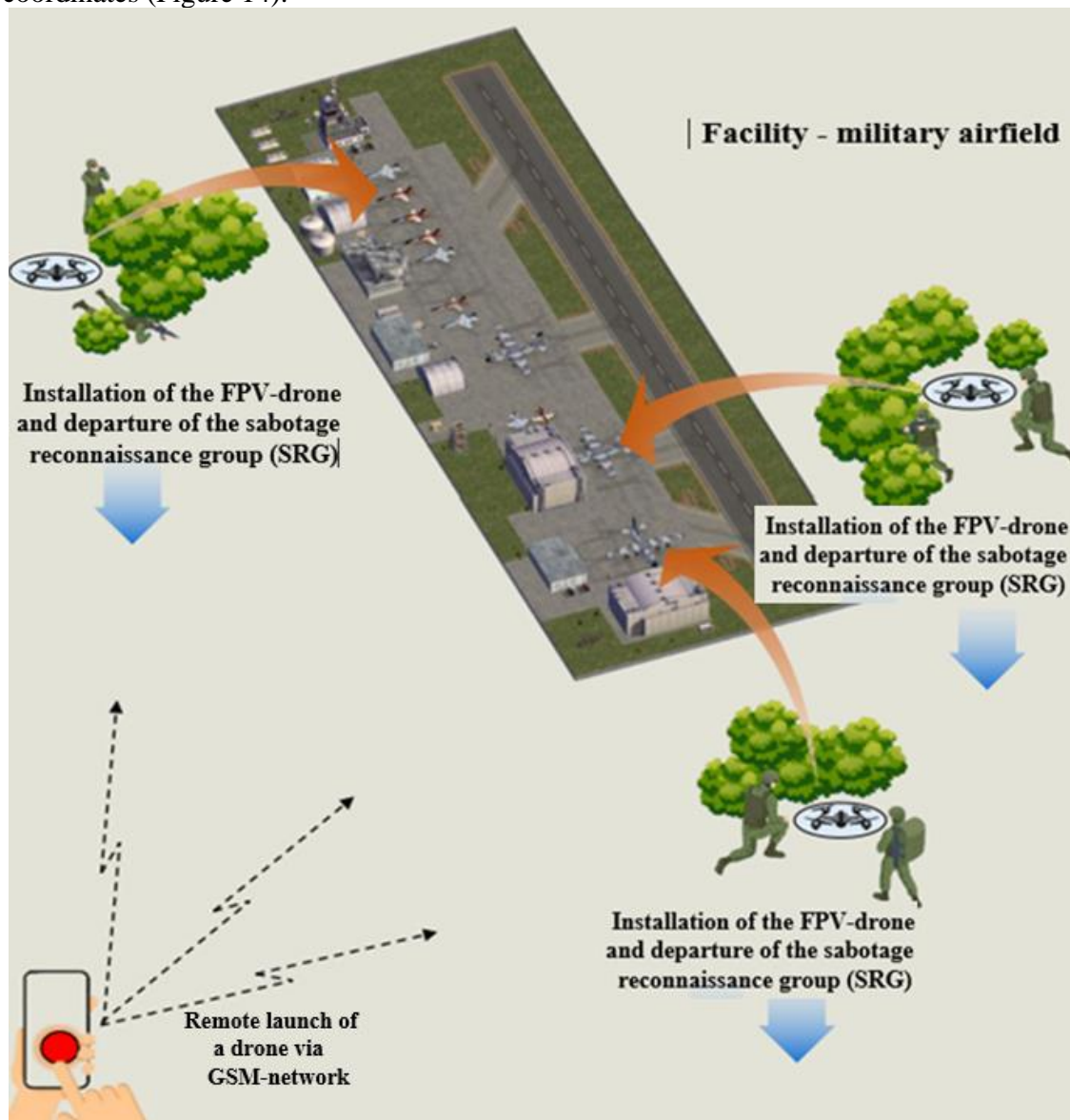


Figure 14. Remote use of FPV drones to destroy important enemy targets

The thirteenth way - increase of the combat radius of FPV drones.

In order to increase the combat range of FPV drones, a 'mother' UAV is used, either an aircraft or a multi-copter type, which also acts as a repeater. Typically, the total payload of such 'mother UAVs' can carry two or three FPVs. The range of their use, depending on the type of 'mother UAV', can be up to 60-70 km. In addition, both ground-based robotic systems and unmanned aerial vehicles (UAVs) can be used as a 'mother UAV' for FPV drones (Figure 15).

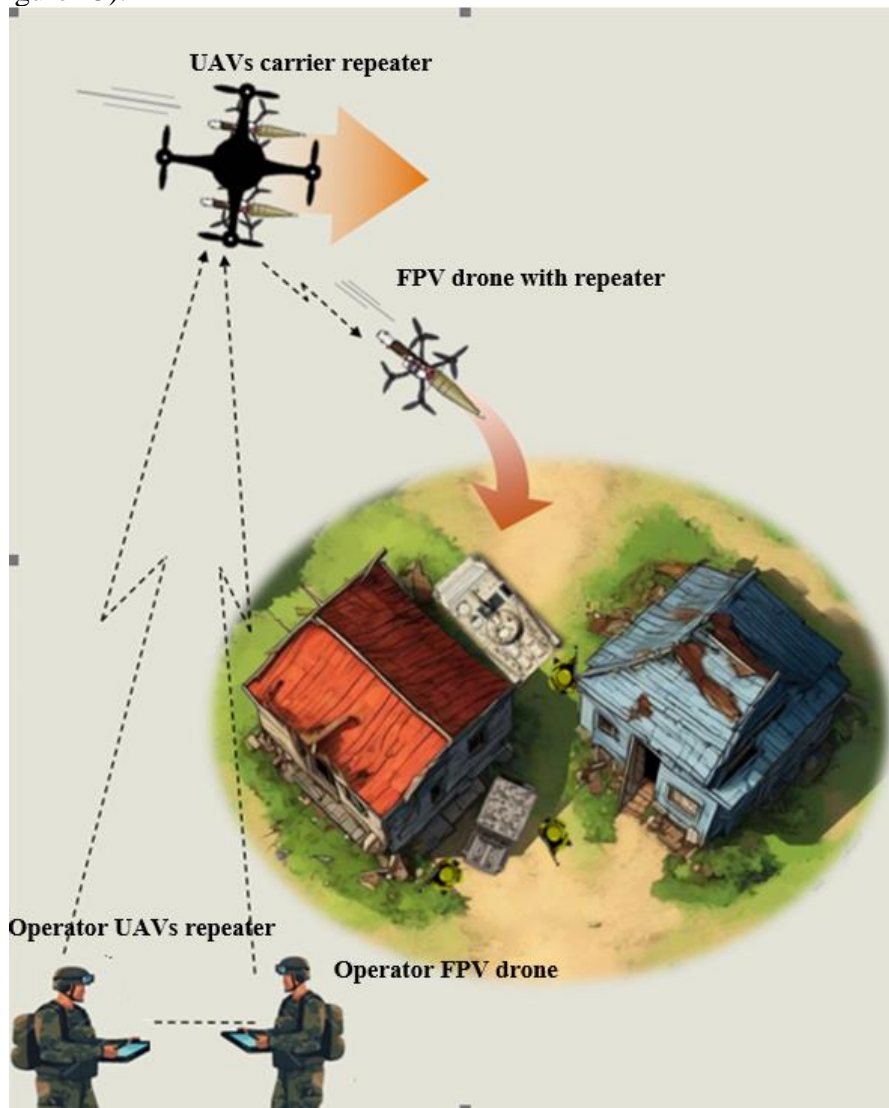


Figure 15. Using a "mother UAVs" to increase the radius of combat use of FPV drones.

The fourteenth way - ensuring the stability of FPV drone control through the use of fibre optic cable.

This method is used in order to ensure stable control of the FPV drone from enemy EW assets and guaranteed target destruction at a range of up to 10 km (in some models up

to 25 km). The experience of using UAVs controlled by fibre-optic cable is being scaled up (Figure 16).

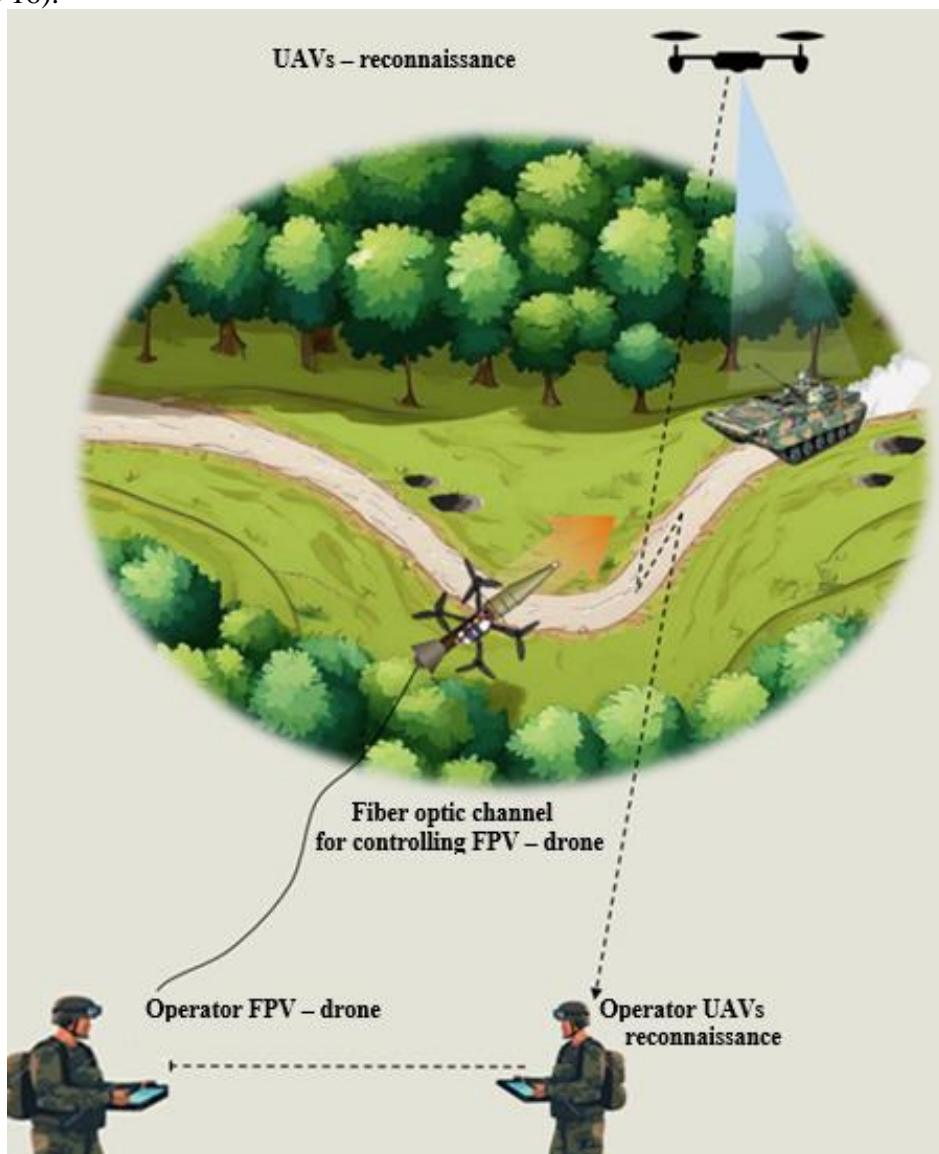


Figure 16. Using fiber optic cable on FPV drones.

It's worth noting that although these drones look like something else, they are a powerful weapon in the right hands. This way of controlling UAVs is definitely not revolutionary, but rather a necessary step in the evolution of drones.

The presence of fibre optics in FPV drones does not add to their striking capabilities or make them more protected from kinetic weapons, such as 12-gauge smoothbore shotguns. Instead, the accuracy of a drone's hit largely depends not only on the stability of its control, but also on the aerodynamic characteristics of the vehicle and the skill of the operator. Therefore, this is definitely not a 'revolutionary' method.

Nevertheless, it is worth noting that a rather characteristic feature of this method is

the clarity of the video to the end point of the route. Application features - preventing sharp manoeuvres, avoiding fire spots along the route.

FPV control on optics is much easier, as the operator does not lose the image to the end point of the route, there is no need for skills to fly through the EW zone and no need to understand the principles of radio horizon. Perhaps the only limitation in the use of such UAVs is the prevention of sudden manoeuvres (changes in direction and altitude) and avoidance of fires along the flight route. It is worth noting that fibre-optic drones are currently even more deadly than conventional FPV drones, primarily because there are no effective countermeasures against them, except for kinetic impact (smoothbore guns, net guns, small arms, etc.).

The fifteenth way - using UAVs to monitor interior spaces.

This method is used in order to detect the enemy and control the interior of a building during assault operations, using micro UAVs with blade protection. Typically, such UAVs have a low weight of up to 50 grams, a limited flight time of up to 4 minutes, and a flight radius. The range of communication within a building is up to 500 metres (Figure 17).

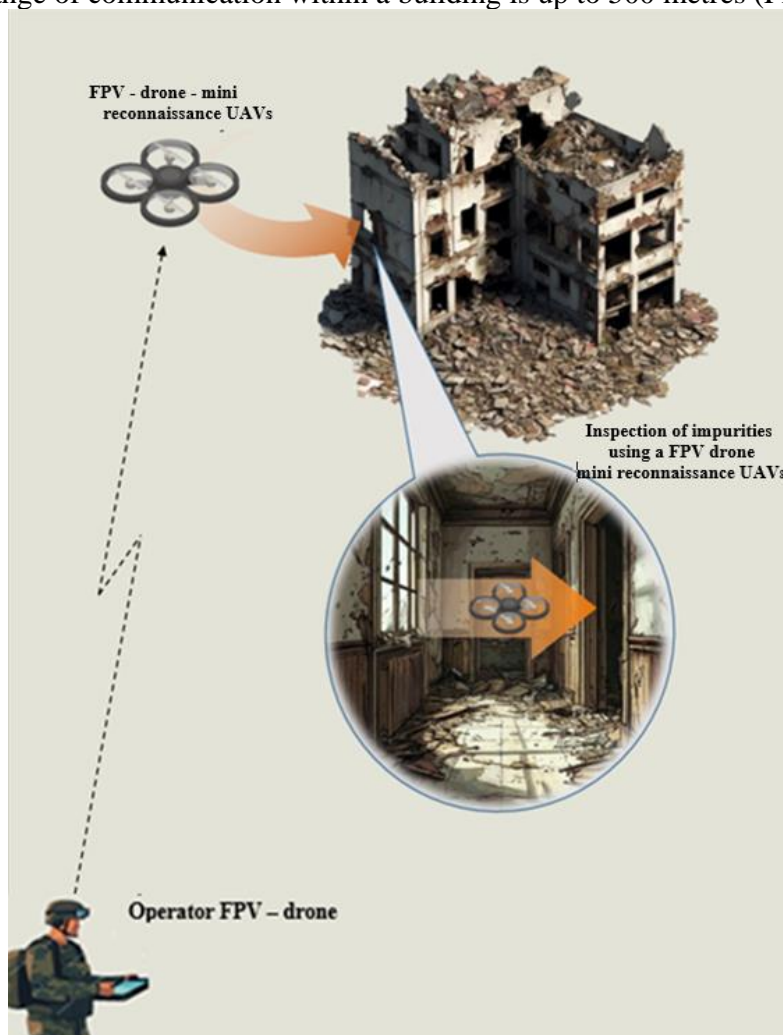


Figure 17. Using UAVs to monitor spaces inside a building.

The sixteenth method - the use of FPV drones for information and psychological influence on enemy personnel.

This method is used in order to reduce the moral and psychological state of enemy personnel and force them to surrender. FPV drones with speakers are sent to the enemy's positions to broadcast sound messages. The hovering height is up to 50 metres (Figure 18).

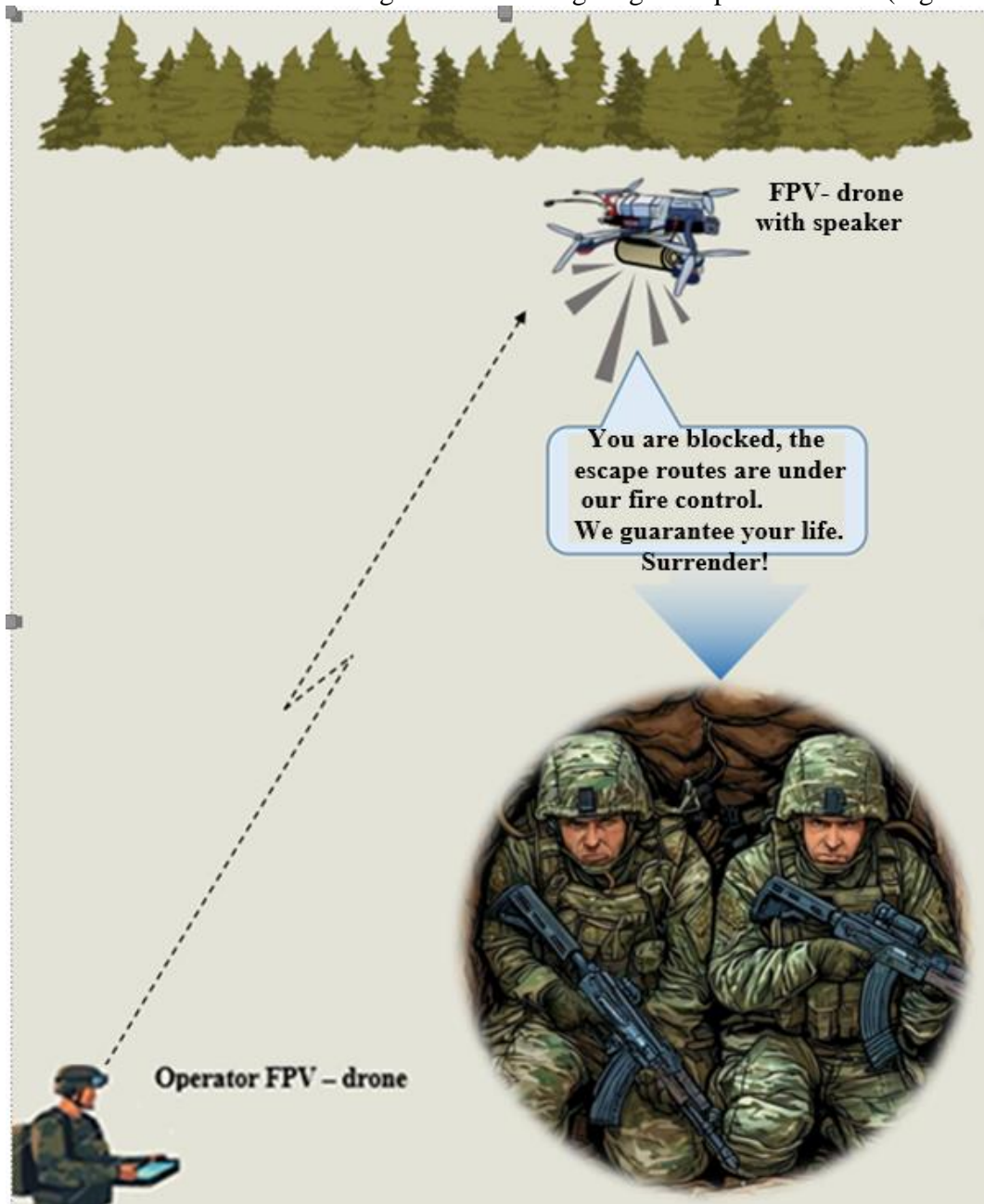


Figure 18. Using drones for informational and psychological influence on enemy personnel.

The seventeenth method - the use of FPV drones for information and psychological influence on enemy personnel and the local population.

This method is used in order to use FPV drone for information and psychological influence on the enemy's personnel and population by dropping leaflets. The weight of printed materials is up to 2 kg (about 200 leaflets) (Figure 19).

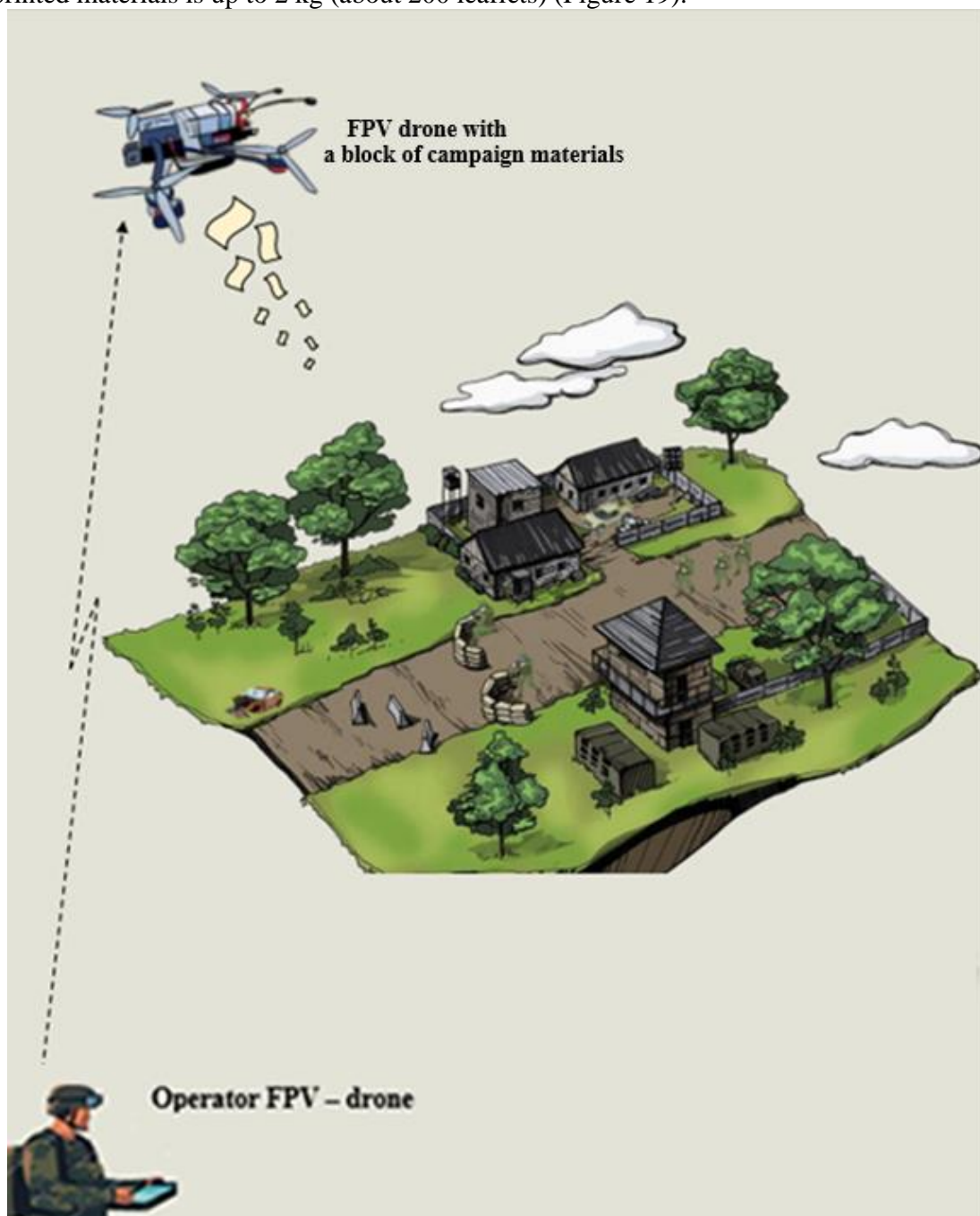


Figure 19. Dropping leaflets – campaign material using FPV – drones.

INFORMATION WAYS TO COUNTER FPV DRONES.

It is worth noting that a feature of modern warfare is the constant threat of air strikes by the enemy, which, as a minimum, results in the detection of personnel and military equipment (ammunition) and, as a maximum, the destruction of personnel or military equipment (ammunition). The widespread use of FPV drones by both sides of the armed conflict leads to the fact that the airspace is saturated with UAVs, which are usually difficult to hide from.

We believe that the tactical techniques, options and information methods of action, practical skills of UAV operators are constantly being improved, and even as we prepare this scientific material, new ways of countering FPV drones are emerging. That is why, in order to preserve personnel, weapons and military equipment, it is necessary to develop at least vigilance and caution and to improve information methods of countering FPV drones as much as possible.

Combating FPV drones requires a comprehensive approach to defence against UAVs in the form of active and passive measures that must be implemented both in the unit and as individual elements by each serviceman.



Figure 20. Division of countermeasures.

In our opinion, it is necessary to specify both active and passive measures to counter FPV drones.

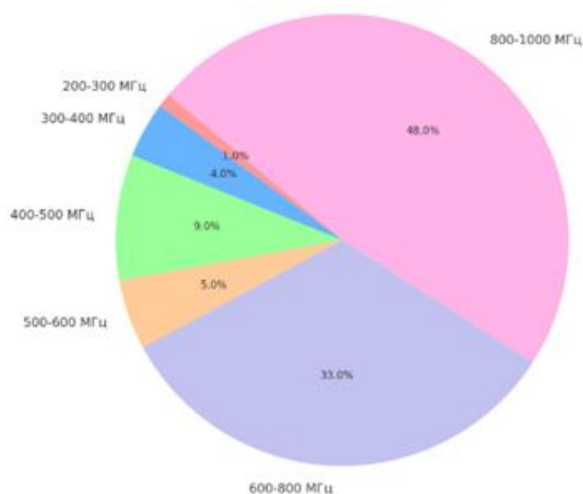
It should be noted that active measures to counter FPV drones include the following:

Firstly, detection and destruction of 'kamikaze' drone operators' calculations (probable launch sites, presence of antennas, specially prepared sites for launching FPV drones, traces of ammunition disassembly, packaging and boxes, inconspicuous cars, repeaters on high-rise buildings and infrastructure elements);

Secondly, early and timely detection of UAVs (visually, by ear, detector or analyser signal) and alerting (receiving a command or notification from a senior observation post, neighbours about the drone in your area of operation).

It is worth noting that standard electronic reconnaissance means do not detect a UAV controlled by an optical fibre cable, as such a drone and its operator's control panel do not use radio communication, the easiest way to detect it is visual or acoustic.

Thirdly, electronic suppression by means of EW (including UAV countermeasures and electronic jamming systems, short-range EWS installed on ground-based unmanned robotic systems) to suppress radio frequencies of control channels and transmission of video and satellite navigation (Figure 1).



Pie Chart 1. Radio frequency range for controlling enemy FPV drones.

It is worth emphasising that the advantages of using EW equipment installed on ground-based unmanned robotic systems (Figure 21) are their high mobility and increased operating time due to the increase in the number of batteries or the placement of a generator on an unmanned platform.



Figure 21. Ground-based unmanned robotic system.

It is worth noting that by actively using electronic warfare means to counter FPV drones and other enemy UAVs (using electronic intelligence (hereinafter referred to as ELINT), ELINT detector of FPV drones "FRANEK", anti-UAV system "SKYWIPER-OMNI" (Figure 22), T-7 electronic jamming complex, anti-drone guns, such as CZECH SOKIL SPS 100 (Figure 23), and THOR short-range EW system (Figure 24)), and not to forget the effectiveness of the joint use of the above-mentioned EW systems and own unmanned aerial vehicles (Reference 8). In view of the above, the priority tasks that should be addressed in the EW ECS as part of the EW CMC and UAVs at command and control points are:

1) minimising ‘friendly fire’ - the integrated use of the Iceberg, Neon and Ocheret systems makes it possible to establish interaction between unmanned aerial vehicles (UAVs) and EWS by transmitting information about their sides to EWS control points, which avoids erroneous suppression actions in areas where friendly UAVs operate;

2) imposing restrictions (prohibitions) in designated flight zones - the Iceberg system allows for joint coordination of UAV and EWS in order to agree on no-fly zones, which allows pilots to plan flight missions more efficiently;

3) introduction of restrictions (prohibited areas of ECM) - the use of the Iceberg system allows for feedback and interaction between EWS units and UAVs to determine "flight corridors" for pilots for a certain period of time with a ban on electronic jamming, which significantly reduces the time and resources required to coordinate joint actions during combat duty;

4) planning of flight missions - the use of analytical data in the Neon and Ocheret systems allows planning a significant number of aerial reconnaissance and fire missions using various types of UAVs (DJI Mavic multi-rotor FPV wing with drops, etc.);



Figure 22. "SKYWIPER-OMNI" UAV countermeasure system.



Figure 23. Anti-drone rifle "CZECH SOKIL SPS 100".



Figure 24. Short-range electronic warfare system "THOR".

Fourthly, reducing the time spent in the probable area of impact due to the speed of the vehicle (an induro motorcycle at a speed of about 80 km/h can cover 5 km in 4 minutes).

Fifth, firepower - destruction of drones by small arms fire, primarily from smoothbore rifles (up to 50 m).

It is worth noting that if it is not possible to stop (destroy) the enemy's attack UAV (FPV drone) attacking the position, one of the options is to use small arms. In the course of research and practical use, 12-gauge smoothbore shotguns (e.g., the Huglu 104 A Silver hunting rifle, 12/76 cm) demonstrated high efficiency (Figure 25). The destruction elements (pellets, buckshot), flying out of the gun's barrel channel, create a cloud that hits the UAV;



Figure 25. Hunting rifle Huglu 104 A Silver, 12 gauge/76 cm

Sixthly, mechanical action - the capture of drones through the use of special devices - 'net launchers' - at short distances (20-30 m).

Seventh, manoeuvre - actions of personnel to evade drone strikes (dispersal of personnel, taking cover, active movement in open areas in case of threat of attack).

Eighth, providing logistics of ammunition, water, and food to units on the LoC through the use of 'heavy drones' and ground-based robotic systems for cargo delivery and evacuation of the wounded.

It should be noted that it is better for personnel to move and hide in the shade of trees and slopes. No sudden movements or running which is very noticeable. Relatively safe weather is dusk, night, fog, rain. Protective anti-drones (Figure 26) will come in handy. As a promising method of countering UAVs, optical effects on the drone's camera are being developed by using a laser device with a wide light beam.



Figure 26. Protective anti-drone cloak.

It is worth noting that in the near future, a promising method of countering UAVs is a rifle that optically affects the drone's camera by using a laser device with a wide light beam (Figure 27).



Figure 27. Optical effect rifle.

It should be noted that passive measures to counter FPV drones include the following:

Firstly, additional fortification of positions (preparation of anti-drone niches and 'holes', bends at the entrance to dugouts and shelters, installation of hinged protective nets and barriers).

Setting up positions is hard work and at the same time the most disguised stage of preparing a unit for a combat mission. In addition to human commotion, there are many other disguising features (fresh soil, new paths, changes in the landscape). Therefore, the

time and place for setting up a position should be chosen carefully.

For instance, it is better to build trenches or carry out other fortification work at dawn or dusk, when enemy aerial reconnaissance activity decreases. At the same time, it is difficult for UAVs to fly in strong winds and rain. At night, the intensity of flights decreases, but at the same time, drones operate more efficiently due to the use of thermal imagers.

When equipping a trench, it is better to equip a side niche at the bottom of the connection path to protect you from FPV drone strikes and UAV drops in case of shelling. It is advisable to make 'L' shaped exits from the dugouts and to equip a second entrance to the shelter (the first one may be destroyed by a strike). When entering the shelter, it is better to use a protective blanket.

It should be noted that the simplest shelter that can be quickly created, camouflaged and used if necessary is a "foxhole" - a small single trench dug at an angle or perpendicular to the trench. This is what makes it possible to quickly take cover if necessary. It also protects you from drops and partially prevents you from being seen from above. A whole network of well-camouflaged "fox holes" at the position will allow you to hide and wait out an air attack. "Foxholes" can also be used as resting places to avoid overcrowding in the dugout. It is advisable to make sure you have as many covered crevices as possible. It is very difficult to see, let alone throw something into such a shelter. The cover conceals the movement of personnel in the trenches and prevents enemy aerial reconnaissance from being able to target them in case of an attempt to drop something into the trench. For this purpose, all materials that can be delivered to the position or found on the spot, up to tightly laid branches, are suitable. All of this must be properly camouflaged. The cover should not only cover the object, but also disguise its outline. That is, from above, even when viewed from different angles, it should be unclear what exactly is hidden there. Another way to secure your positions is to cover them with nets that allow you to capture everything that is dropped from the drones.

Secondly, camouflage of positions and equipment (installation of camouflage nets with irregular geometric shapes with a distance of 0.3-0.5 m to the equipment in the shade of trees and bushes, inside destroyed buildings, use of heat-protective capes, control of demasking features from a drone).

Thirdly, the creation of false positions (equipped with heat and light sources) with the installation of models of military equipment and vehicles (including those unsuitable for operation) and simulation of their activities.

Fourthly, the installation of protective nets (screens) made of fishing nets on the routes of rotation, evacuation of personnel, delivery of ammunition, water and food;

Fifthly, installation of hinged protection elements (visors, canopies) and 'dome' EWS on vehicles;

Sixthly, taking into account weather conditions, terrain and time of day when planning active operations and movements;

Seventh, setting up aerosol curtains, creating fires of smoke at positions (objects) and routes of movement (including false ones).

As a conclusion of this study, we note that in modern combat conditions, the use of UAVs is growing exponentially. It is the constant combat duty of drones in the air that has led to the decentralisation and reduction of troops on the front line. It is worth noting that the basic tactics of defensive combat, which used to involve a platoon, are now being

handled by a squad. Where there used to be a 'squad stronghold', there are now three 'holes' of 2 people each. Both sides seek to minimise the movement of combat personnel. One 'armour' can involve up to a dozen UAVs, or 'birds' as they are colloquially known, and 2-3 drones will be involved in the pursuit of a soldier. In the LoC area, reconnaissance drones, bombers and FPV teams are on standby in their respective sectors in shifts. Some are searching, others are striking.

That is why we believe that it is advisable to distinguish recommendations for personnel on the information basis of options for countering unmanned aerial vehicles (UAVs) of the FPV type in combat conditions, which we divide into three large groups: camouflage, fortifications and logistics, actions when a drone is detected.

Recommendations for disguise measures include:

Disguise yourself from observation from the air, use canopies, nets, branches, grass, leaves. It should be noted that the following can demask positions: plastic wrap, white bags, household waste, fresh ground, movement of personnel.

From the air, personnel are less visible if they: are not moving; are in the shadow of buildings (objects); are sitting rather than lying down (reduced size); and are in the same colour as the terrain, i.e. do not fuss.

It is advisable to move and hide in the shade of trees and slopes. Do not make sudden movements or run - it is noticeable. It should be noted that the relatively safe time for personnel to move in such weather conditions as dusk, night, fog, rain. It is advisable to use protective capes ('cloaks').

It is advisable to place and camouflage equipment in forest belts, along (inside) hangar buildings, change its location, and equip simple camouflaged sheds. Particular attention should be paid to covering the glass of vehicles that reflects. If the enemy is in the north, it is advisable to place the equipment behind a building on the south side.

We believe that vehicles should not be placed near the positions, putting them in a hidden place for quick access. Collect all garbage in bags and a separate pit. Scattered ration packs, cans, plastic bottles, and polyethylene perfectly demask the position. To monitor camouflage 'quietly', launch your drone and inspect the area for any demasking features.

Camouflage nets are always needed in large quantities. When installing them, change their configuration, the more obscure and blurred the silhouette, the harder it is to detect the object. Satellite dishes get hot, so they should be hidden in a hole and masked from both daytime and thermal imaging cameras.

It is advisable to create false positions with demasking features. Install models of military equipment or disabled vehicles. Simulate their activity. Start fire in empty shelters at night, place trench candles.

It's worth noting that at night, you should use light camouflage. Fire from a cigarette, campfire, flashlight, headlights, phone screens - attracts drones like moths to a flame.

Direct speech: 'Pro-life conversations are only allowed in the shelter. You don't need to 'huddle up' with cigarettes if you're bored. Do not stand around idly. If you are called on command, warn another soldier.'

The main criterion for the enemy to detect you from the air is movement during the day and heat glare at night. You should keep quiet, try to communicate in whispers and gestures, and listen to sounds.

Recommendations for fortification and logistics include:

When equipping a trench, make a side niche at the bottom to protect from debris during shelling, FPV strikes and ammunition drops. Make the exits from the dugouts in the shape of the letter 'L'. Hang a protective cover at the entrance to the shelter. Set up a second entrance to the dugout (the first one may be destroyed by a shelling).

As an obstacle for FPV drones, prepare and fix corded anti-drone curtains made of 4-5 mm thick ropes in front of the positions: length - 6 m, height - up to 4 m, interval between hanging ropes - 20 cm.

Another option for protection is to install screens made of cheap fishing nets (length - up to 80, height - 4 m.) - they are invisible to the operator, equip additional canopies and visors.

We believe that it is advisable to prepare and install smoke grenades in advance at the position (at a distance of 20-30 metres) to activate them in case of a threat of kamikaze attacks. Each of the soldiers has hand-held smoke grenades of instant action.

It is the presence of additional protection elements on the vehicles ('visors', 'grills', shields, nets, chains, anti-shrapnel protection in the form of 1 cm thick rubber pieces on 'screws') that will increase the survivability of the crew and passengers when attacked by FPV drones. The main thing is not to overdo it.

In our opinion, the most desirable and ideal version of electronic warfare equipment at the platoon position is a spectrum analyser and UAV detector, a device for intercepting video images from FPV drones, a portable broadband 'dome' electronic suppression system, and individual mobile 'suppressors'.

As of 01.02.2025, it is a military lucky day in Ukraine to buy a well-proven EWS drone suppressor.

In order to combat 'hunters' for aircraft-type UAVs, it is necessary to install onboard electronic warfare equipment on the vehicles.

In our opinion, if there is any other way to influence the transmission channel of the video image of an enemy FPV drone, we believe that an FPV monitor or goggles that search for the transmission channel (usually 5.8 GHz) can be used to detect it. The video transmitter of the FPV drone is set to the same channel and maximum power. After launch, interference is created to control the video transmission channel (drones 'work' on the same frequency).

We believe that mechanical robotic unmanned platforms and 'heavy' drones to provide logistics of ammunition, water, food and evacuation of the wounded significantly reduce the loss of personnel from FPV drones.

It is worthwhile to use active actions when detecting an FPV drone. It is always advisable to listen to the sounds and feel the "sky". First, detect by sound (it's better to hear at night), then visually. Spread your ears like Cheburashka and keep your eyes open. Report in a timely manner. Treat all UAVs as hostile.

We believe that it is quite progressive to learn to distinguish a Mavic from an FPV by its sound. The former is quieter and smoother, while the latter is shrill and has sharp drops when accelerating.

In order to increase security, the movement should be carried out (by time and place) on the basis of an analysis of the enemy's drone activity in a particular area of hostilities (the enemy knows about the 'grey' time).

It is advisable to avoid positions and move along the trenches, and in a settlement - from building to building. The interval in the 'trio' is at least 5 metres. It is advisable to

move secretly in triplets to a control point (shelter).

The scout drone is the harbinger of FPV. If you spot an enemy UAV in motion (including in a car), do not lead it to your forces. Take cover, wait, watch and do not reveal the position of your unit. When in trench, lean against a tree trunk and do not move.

Personnel actions in case of detection of an FPV drone:

Always control the 'sky' by sectors when moving. It is worth remembering that it is advisable to keep a distance and notice the nearest shelters (destroyed buildings, 'holes', trenches bushes, etc.) for a 'dash' in case of a threat of FPV drone attack. A shell crater can be a 'safe place'. It should be noted that it is not advisable to concentrate in one place. The main priority is dispersal, rapid manoeuvre and speed of each soldier.

It should be noted that if a soldier hears an FPV drone, it is advisable to move to cover as quickly as possible. If the personnel are in position, it is advisable to make sudden, sharp movements.

If an FPV drone is in the immediate vicinity (20-30 m), you should not try to 'freeze', hoping that it will not notice and fly by. It is advisable to escape by moving towards a natural shelter (hill, forest belt, bushes, etc.). Rescue itself is about rapid reaction and fast movement.

Small arms fire itself is ineffective (small target size, high speed). In addition, when you shoot, you are static, which makes it easier for the operator to aim the drone. At close range (up to 50 m), a shooter (preferably two) with hunting or pump-action rifles has a chance. For their preparation, they should train with 'plates'.

In today's realities of combat, there are cases of the operator playing with the 'victim'.

If you are agile and skilful in dodging, hiding behind cover (a 40 cm tree trunk is also an option), and are able to attack an FPV drone by throwing a stick or other objects, your chances of survival increase. However, when driving a vehicle, it is advisable to focus special attention and control from the 'sky' on the perimeter from the rear and flanks (up to 80% of FPV drone attacks are on the rear and side of the vehicle).

It is in dangerous areas that we believe it is advisable to move at the highest possible speed. Do not choose long routes. If you see a FPV drone, it is advisable to pull over (preferably into a forest), stop and quickly concentrate. There is little chance of avoiding an FPV drone by following the road.

It is worth noting that when the vehicle stops, everyone leaves the vehicle very quickly, no one argues about who gets out first or unloads ammunition, as the threat of death increases. As the practice of combat shows, time is against you.

The survival and logistics of cargo in the combat zone facilitates the use of high-speed motorcycles such as induros, buggies, and ATVs with trained drivers. It is worth noting that electric motorcycles ensure silent movement and a higher sensitivity of drivers and passengers to early detection of drones by sound.

We believe that extreme driving requires experienced driver training. It is day and night training that will allow a future driver to identify and remember landmarks during the day and then find them at night.

It should be noted that if the personnel detect an FPV drone on the ground (especially if it squeaks near their positions), they should not run towards it with fingers outstretched, hoping for a new trophy. As a rule, this is a 'trap'. Do not approach from the camera side, as the enemy operator is waiting for the personnel to appear in the frame), do not touch,

mark, it is advisable to report to the commander who will give the command - a specialist miner who will deal with the situation.

It is worth noting that the technical leap in the use and adaptation of FPV drones to the modern theatre of operations has led to a significant expansion of the range of combat missions performed by them.

The demand of combat units for trained and equipped 'kamikaze' drones exceeds the supply on the 'war' market. The innovative development of this type of weapon will undoubtedly entail the search for and implementation of new technical solutions and countermeasures (electronic, optical, mechanical, etc.), and will lead to the creation of separate structural units (calculations) for both their use and countermeasures.

We believe that in the near future, certain elements of information counteraction to UAVs of the FPV type - drones - will affect every serviceman and combat units. Competitions in the drone-anti-drone category are just beginning.

Reference:

FPV - drones and their role in the Russian-Ukrainian war. (2025). URL: <https://surl.li/kqvuoo> (date of access 28.03.2025)

The Evolution of FPV Drones. What Innovations Have Appeared During a Full-Scale War. (2025). URL: <https://surl.li/tfqbvvn> (date of access 01.04.2025)

CHAPTER 4. MODERN BASES OF FORMING AND ENSURING CYBERSECURITY AS A BASIS OF NATIONAL SECURITY: INTERNATIONAL PRACTICES

Victor BESCHASTNYY

Head of Secretariat of the Constitutional Court of Ukraine,

Doctor of Science of Law, Full Professor,

Honored Lawyer of Ukraine,

beschastnyy.vm@gmail.com

<https://orcid.org/0000-0002-4650-7371>

Abstract. The research analyses the world models of cybersecurity formation and ensuring. It is noted that in the United States, cyberspace is doctrinally assigned the status of the fifth theatre of war (along with land, water, air and space). It is found that most European countries, especially those that are members of the NATO bloc, have also developed their own cybersecurity strategies. The main constituent elements of cybersecurity in Asian countries (China, Thailand, Japan) are noted. It is proved that the national cybersecurity strategies and bloc doctrines of the Western world do not reflect the international community's concern in preventing the next round of the arms race at a qualitatively new level of development of information and communication technologies, reducing the risk of aggressive use of these technologies for the violent resolution of criminal acts in the global information space. The main priority for the development of the cybersecurity system is the formation of cyber troops and special public authorities that ensure cybersecurity in the national security system. It is noted that one of the priority steps should be the development and adoption at the level of the United Nations of a document that establishes the fundamental principles of activities in the global information space, as well as ensuring the security of these activities.

Keywords: cybersecurity, cyberspace, global information space, security, information and communication technologies

СУЧАСНІ ЗАСАДИ ФОРМУВАННЯ ТА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЯК ОСНОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ: СВІТОВИЙ ДОСВІД

Анотація. У дослідженні здійснено аналіз світових моделей формування та забезпечення кібербезпеки. Зазначено, що у США за кіберпростором доктринально закріплено статус п'ятого театру військових дій (поряд із сушею, водою, повітрям та космосом). З'ясовано, що більшість європейських країн, особливо тих, що входять до блоку НАТО, також розробили свої стратегії кібербезпеки. Зауважено про основні складові елементи кібербезпеки в країнах Азії (Китай, Таїланд, Японія). Доведено, що у національних стратегіях кібербезпеки, блокових доктринах країн західного світу слабо виражено занепокоєння міжнародного співтовариства в питаннях недопущення чергового витка гонки озброєнь на якісно новому рівні розвитку інформаційно-комунікативних технологій, зниження небезпеки загрози агресивного використання цих технологій для силового

вирішення злочинних діянь у глобальному інформаційному просторі. Головним пріоритетом розвитку системи кібербезпеки є це формування кібервійськ і спеціальних органів державної влади, що забезпечують кібербезпеку в системі національної безпеки. Зазначено, що одним із першочергових кроків має стати розроблення та ухвалення на рівні Організації Об'єднаних Націй документа, який закріплює фундаментальні засади діяльності у глобальному інформаційному просторі, а також забезпечення безпеки цієї діяльності.

Ключові слова: кібербезпека, кіберпростір, глобальний інформаційний простір, безпека, інформаційно-комунікативні технології.

Вступ. Динамічне формування глобального інформаційного простору пов'язане, з одного боку, з наданням людству небачених раніше інформаційних можливостей, з другого – з виникненням нових загроз. З'явився новий феномен – «кібербезпека», з яким пов'язані такі поняття, як «кіберзлочинність», «кібертероризм», «кібервійни». Організація безпечного функціонування національних інформаційних інфраструктур, швидше за все, визначатиметься відповідними концепціями кібербезпеки, розробленими майже всіма розвиненими країнами світу та великими міжнародними організаціями.

Кібербезпека є вкрай актуальною у сучасному світі, оскільки цифрові технології проникли у всі сфери життя, а кібератаки стають дедалі складнішими та небезпечнішими. Кількість загроз, таких як фішингові атаки, шкідливе програмне забезпечення, DDoS-атаки та атаки на критичну інфраструктуру, невпинно зростає, що створює загрозу для державних органів, бізнесу та громадян. Особливо важливим аспектом є кібербезпека як частина національної безпеки, адже кібершпигунство, інформаційна війна та навіть кібертероризм активно використовуються різними державами для досягнення геополітичних цілей. Яскравим прикладом є агресія Росії проти України, яка включає не лише військові дії, а й масовані кібератаки на урядові та стратегічні об'єкти.

Водночас питання захисту персональних даних набуває особливого значення, оскільки цифровізація охоплює фінансовий сектор, соціальні мережі та інші онлайн-сервіси, а витік конфіденційної інформації може призвести до фінансових втрат та маніпуляцій із даними користувачів. Бізнес також у зоні ризику, адже кібератаки можуть спричиняти значні збитки через викрадення даних, промислове шпигунство або вимагання викупу за розблокування систем. У зв'язку з цим міжнародна спільнота активно розвиває співпрацю у сфері кібербезпеки, створюючи такі ініціативи, як НАТО Cooperative Cyber Defence Centre of Excellence, Європейське агентство з кібербезпеки (ENISA) та Будапештську конвенцію, які спрямовані на об'єднання зусиль у боротьбі з кіберзлочинністю. Окремим викликом стає розвиток штучного інтелекту та Інтернету речей, оскільки розумні пристрої, такі як камери, автомобілі з автопілотом і медичні девайси, можуть ставати мішенню для хакерів. Загалом кібербезпека є не просто технічним питанням, а необхідною складовою захисту держав, бізнесу та суспільства загалом. Для ефективного протистояння кіберзагрозам потрібно постійно вдосконалювати технології захисту, навчати населення цифрової грамотності, розвивати міжнародну співпрацю та підтримувати фахівців, які займаються кіберзахистом. У сучасних умовах захист інформаційного простору є

важливим елементом безпеки кожної країни, особливо у контексті гібридних воєн та цифрових загроз, кількість яких невпинно зростає.

1. Формування та розвиток кібербезпеки у США.

Глобальний інформаційний простір можна розглядати як сукупність взаємозалежних інформаційних інфраструктур різного рівня (міжнаціональних, національних, регіональних та інших). Основа глобального інформаційного простору – мережа Інтернет. Формування глобального інформаційного простору породило такі загрози, як кіберзлочинність, кібертероризм, загрози військово-політичного характеру, що проявляються у застосуванні інформаційно-комунікаційних технологій для досягнення політичних, економічних, військових цілей за допомогою ворожого використання цих технологій, а також такі загрози, як:

- неправомірне використання інформаційних ресурсів іншої держави без узгодження з нею;
- дії в інформаційному просторі для підризу політичної, економічної та соціальної систем іншої держави, психологічна дезінформація населення, що дестабілізує суспільство;
- маніпулювання інформаційними потоками в інформаційному просторі інших держав, дезінформація та приховування інформації задля спотворення психологічного та духовного середовища суспільства, ерозії традиційних культурних, моральних, етичних та естетичних цінностей;
- інформаційна експансія, отримання контролю за національними інформаційними ресурсами іншої держави.

Реалізація цих загроз, що так чи інакше пов'язана з кібервійнами та проведенням спеціальних операцій в інформаційному просторі, може призвести до порушення миру та безпеки, підризу довіри в міжнародних відносинах, а також негативно впливає на цілісність державних інфраструктур та заподіює неприпустимі шкоди. Це визначає потребу у відповідній протидії. Основою для формування стратегічного вектора в організації такої протидії покликані стати існуючі та розроблювані концептуальні документи в галузі кібербезпеки.

Кібернетичну могутність держави (*cyberpower*) США розглядають сьогодні як здатність використовувати кіберпростір у своїх інтересах для створення в ньому переваг і можливість впливати на ситуацію в інших операційних середовищах (військовому, військово-політичному, економічному, інформаційному) (*Cyberpower, 2009*). Кібернетична могутність держави у військово-політичній сфері визначається у доктринальних документах США як застосування стратегічних та оперативно-тактичних планів та концепцій, які, у свою чергу, використовують інструменти кіберпростору для досягнення військово-політичних цілей та виконання військових місій.

Використання кібернетичної могутності держави американці розглядають у зв'язку з адекватним і зваженим (на їхню думку) використанням м'якої та жорсткої сили у шести основних фазах.

Фаза 0. Формування стратегічних та оперативно-тактичних цілей.

Фаза 1. Стимування агресії.

Фаза 2. Захоплення ініціативи та забезпечення свободи власних дій.

Фаза 3. Здійснення стратегічних та оперативно-тактичних операцій і досягнення повної переваги.

Фаза 4. Перехід до операцій із встановлення стабільності, безпеки та верховенства закону.

Фаза 5. Участь у відновленні економіки та передачі управління до цивільної влади.

Концепція кібернетичної могутності держави передбачає, що основою майбутніх військових стратегічних операцій (2012–2025 рр.) буде реалізація таких трьох видів специфічних дій:

1) встановлення, розширення та забезпечення досяжності потенційного супротивника, як віртуальними – через кіберпростір, так і фізичними – звичайними засобами;

2) отримання, вдосконалення та об'єднання знань про кіберпростір;

3) ідентифікація, створення та ефективне використання різних властивостей кіберпростору.

Загалом США вважають кібернетичну могутність фундаментальним явищем сучасного життя. У політичній, економічній та військовій сферах інформаційно-комунікативні технології мають забезпечувати та підтримувати діяльність ключових елементів американської інфраструктури, зокрема й у галузі національної безпеки. Вважається також, що Сполучені Штати повинні створити ефективну національну та міжнародну стратегічну основу для розвитку та використання своєї кібернетичної могутності як повномасштабний напрям реалізації стратегії національної безпеки. Така стратегічна основа матиме структурні та геополітичні складові. Структурна складова зосередить свою увагу на зміцненні безпеки та людському капіталі, поліпшенні управління й більш ефективній організації діяльності. Геополітична – на більш традиційній сфері забезпечення національної безпеки та обороноздатності США. Сюди належать (Скорик, 2020):

- розвиток концепції мережевоцентричних операцій;
- інтегроване планування комп'ютерних мережевих атак;
- розширення ефективних способів впливу на стан та характеристики кіберпростору;
- грамотне поєднання планування діяльності в кіберпросторі з плануванням діяльності звичайних збройних сил та установою відповідно до цієї доктрини;
- освіта і навчання в галузі інформаційних технологій та інформаційної безпеки;
- міжнародна діяльність у цих галузях.

Особливе місце в концепції кібернетичної могутності держави відводять інформаційно-комунікативним технологіям, які сьогодні можуть значно збільшити ймовірність успіху в операціях із забезпечення стійкості, безпеки, переходу до мирного життя та відновлення (операції SSTR). Такі технології американські стратеги виділяють як основну частину будь-якої військової місії. Є п'ять основних складових ефективного використання інформаційно-комунікативних технологій: 1) гарантоване (американським урядом) спільне використання інформаційно-комунікативних технологій цивільного та військового призначення під час проведення операцій SSTR; 2) обов'язкове використання військових інформаційно-комунікативних технологій під час планування та проведення операцій SSTR; 3) попереднє

планування та встановлення партнерства у галузі інформаційно-комунікативних технологій з іншими регулярними учасниками операцій SSTR; 4) зосередження уваги на країні, де проводять операції SSTR; 5) використання ключових можливостей інформаційно-комунікативних технологій для підтримки основної стратегії дій.

Нині Америка активно опрацьовує питання створення кібервійськ. У Міністерстві оборони США як найпотужніший організації в галузі кібербезпеки вже існують такі підрозділи, що проводять операції (як оборонні, так і наступальні) у кіберпросторі:

- мережеве командування (відповідає за безпеку домену .mil);
- підрозділи ВМС США з проведення операцій у комп'ютерних мережах;
- *Cyber Task Force* у структурі ВПС США;
- командування C4 (*Command, Control, Communications and Computer*) корпусу морської піхоти.

Створюють кіберкомандування як орган, що координує діяльність усіх підрозділів, відповідальних за питання кібербезпеки у структурі міністерства оборони, а також здійснює оперативну взаємодію з іншими відомствами (поза міністерства оборони). При цьому не йдеться про створення кібервійськ як окремого виду збройних сил.

Серйозними проблемами розроблення стратегії дій кібервійськ є (*Стежко, 2021*):

- проблеми ідентифікації у мережі джерела нападу;
- проблеми законодавчого розподілу актів кіберзлочинів, кібершпигунства та військового кібернападу;
- проблеми оцінки ефективності та достатності фінансових витрат при забезпеченні кібербезпеки та, як наслідок, проблеми бюджетного планування.

Фахівці Міністерства оборони США зазначають, що державні відомства стикаються з тими самими проблемами у сфері кібербезпеки, як і бізнес-структури (при цьому має місце формула «однакова атака – різні наслідки»). Як наслідок гостро постає питання про залучення кадрів вищої кваліфікації (на тлі світового рівня) для роботи в галузі кібербезпеки на користь державних відомств. І тому розробляють окрему федеральну програму, яка покликана вирішити питання кадрового забезпечення кібервійськ.

Під час розроблення стратегії ведення кібервійн фахівці США категорично відкидають використання принципу стримування, який спрацьовував у період ракетно-ядерного протистояння часів «холодної війни». Основна причина в тому, що в кіберпросторі відсутня абсолютна впевненість у надійному придушенні противника та використання принципу стримування може призвести до небезпечних ілюзій у політиків. Національна стратегія кібербезпеки США, швидше за все, будуватиметься на принципах управління ризиками, тобто балансу потенційних загроз і витрат на їх нейтралізації.

В основу ідеї створення кібервійськ закладено одну із складових концепції кібернетичної сили держави – концепцію військової кіберсили (*Military CyberPower*) (*Military, 2009*). При цьому військову кіберсилу розглядають як один із станів кіберпростору стосовно виконання військових місій і кампаній, включно з гуманітарною допомогою, ліквідацією наслідків (операції *HA/DR*), забезпеченням

стійкості, безпеки, переходом до мирного життя і відновленням (операції *SSTR*), а також військовим управлінням, управлінням персоналом, військово-медичним та матеріально-технічним забезпеченням.

Особливого значення в концепції військової могутності надано забезпеченню збройних сил сучасними інформаційно-комунікативними технологіями та інформаційно-телекомунікаційними мережами, збалансованому використанню м'якої (в основному з використанням елементів кіберпростору) та жорсткої сил під час виконання військових місій, зв'язку з партнерами по коаліціях. Також велике значення надають ефективному управлінню ризиками під час проведення військових операцій, оскільки дедалі збільшується залежність військової інфраструктури від «цивільних елементів» кіберпростору, їх можливостей, продуктів інформаційно-комунікативних технологій і служб.

Одна з основних складових військової кіберсили – це операційне середовище, що містить інформаційні операції (операції *IO*), операції впливу (в основному – операції з використанням «м'якої сили»), мережевоцентричні операції (операції *NCO*), розвідувальні операції та операції, пов'язані з комерційним та адміністративним використанням кіберпростору (*Литвиненко, 2017*).

Крім того, концепція військової кіберсили розглядає ідею інтеграції мереж Міністерства оборони США через об'єднання існуючих методів, мережевих послуг і сервісів для створення глобальних інформаційних ґрат (*Global Information Grid, GIG*) – як загальної мережевої основи для реалізації мережевоцентричних операцій у кіберпросторі. Такі мережеві ґрати створюють у межах програми формування об'єднаної корпоративної регіональної системи обміну інформацією (*Combine Enterprise Regional Information Exchange System, CENTRIXS*).

Концепція також розглядає різні військові сценарії, які полягають у можливості ведення різних інформаційних операцій, воєн, зокрема мережевоцентричних, асиметричних та іррегулярних.

Так, у США кібербезпеку регулює складний комплекс федеральних законів, галузевих федеральних законів, загальних законів штатів та галузевих законів штатів, а також норм загального права, які еволюціонували в результаті судових рішень (*Cybersecurity, 2022*). Загальні федеральні закони регулюють обмін інформації з урядом та конкретні дії, такі як комп'ютерний злам або незаконне перехоплення електронних повідомлень, тоді як інші федеральні закони диктують особливі правила, які можуть бути застосовні лише до певних компаній у критично важливих секторах інфраструктури, таких як охорона здоров'я та фінансові послуги.

Міністерство внутрішньої безпеки США (*Department of Homeland Security, DHS*) у 2018 році опублікувало нову кіберстратегію, яка визначила дії *DHS* на п'ятирічний період (*National Cyber, 2018*).

Ця стратегія національної безпеки США містить п'ять «стовпів» управління ризиками кібербезпеки, які є актуальними не тільки для забезпечення національної кібербезпеки Америки, а також для формування міжнародно-правового режиму кібербезпеки:

1. Розуміння прогресуючої природи загроз із боку інших країн та приватних осіб;
2. Захист федеральних мереж та секторів критичної інфраструктури;

3. Протидія транснаціональним кримінальним хакерським угрупованням;
4. Покарання держав за зловмисні кібердії;
5. Просування у глобальному масштабі найкращих практик кібербезпеки.

12 жовтня 2022 року було опубліковано нову редакцію Стратегії національної безпеки США (*Biden-Harris, 2022*). Ця стратегія також торкається питань кібербезпеки. За словами радника з національної безпеки Дж. Саллівана, ця стратегія «виходить із передумови, що дві стратегічні проблеми – геополітична конкуренція та спільні транснаціональні небезпеки – взаємопов'язані» (*Remarks, 2022*). Проголошують основні цілі: безпека американського народу, розширення економічних можливостей та захист демократичних цінностей.

Для досягнення цих цілей США мають намір:

- інвестувати в інструменти та важелі американського впливу;
- створити найсильнішу з можливих коаліцію держав для колективного впливу задля формування глобального стратегічного простору;
- модернізувати та посилити армію для готовності до епохи стратегічного суперництва.

Невід'ємною складовою американської політики є підвищення обізнаності інших країн про можливі ризики, а також розвиток їх механізмів захисту від електронних загроз середовища, особливо тих, що зароджуються всередині власних кордонів. Допомога передбачає: консультації щодо захисту мереж; навчання та сертифікацію фахівців із кібербезпеки; створення первинних груп швидкого реагування та нарощування ресурсів у мережевих операційних центрах та службі безпеки центрів обробки даних.

США також надають допомогу в межах двосторонніх відносин із членами НАТО та країнами, що розвиваються по всьому світу, оскільки ці країни виявили інтерес у підвищенні власного рівня кібербезпеки. Так, у межах здійснення своїх міжнародно-правових зобов'язань США впливає на формування програм НАТО з кібербезпеки. Зокрема, забезпечує військову кібербезпеку, захист інформації про розташування складів, найменування зброї та дані військовослужбовців. Америка надає НАТО підтримку від звичайних хакерських атак. На користь удосконалення навичок особового складу кіберпідрозділів та проведення бойового злагодження з країнами НАТО на регулярній основі проводять спільні навчання. Найбільшим із них стало *Cyber Coalition 2021*, проведене наприкінці 2021 року за безпосередньою участю близько тисячі фахівців кіберпідрозділів Північноатлантичного альянсу та країн-учасниць угоди «Партнерство заради миру» (Ірландії, Фінляндії, Швейцарії та Швеції). Мета навчання – підвищення можливості військового союзу протидіяти загрозам у кіберпросторі (*Cyber coalition, 2021*).

Отже, реалізована в США система забезпечення кібербезпеки, починаючи з готовності до протистояння кіберзагрозам і їх запобігання або усунення, дає змогу ефективно протистояти численним кіберінцидентам різного ступеня складності.

Вибудована та функціонуюча система суб'єктів забезпечення кібербезпеки охоплює багато напрямів потенційних кіберзагроз. Законодавче регулювання та наукове забезпечення дають змогу успішно впоратися з широким спектром загроз та небезпек.

Вивчений досвід забезпечення кібербезпеки в одній із найбільш розвинених у цьому напрямі державі, безумовно, може бути корисним для вітчизняних науковців

та юристів-практиків працівників у розробці перспективних наукових досліджень, методик та рекомендацій щодо вдосконалення правового й організаційного забезпечення вищого рівня кібербезпеки в сучасній Україні.

2. Європейський досвід реалізації заходів кібербезпеки.

Аналізуючи стратегічні документи в галузі кібербезпеки європейських країн, можна зробити такі висновки.

У середовищі, де постійно з'являються та еволюціонують кіберзагрози, країни-члени Євросоюзу при зустрічі з новими глобальними загрозами мають намір отримати велику вигоду від гнучких, оперативних стратегій кібербезпеки. Транскордонний характер загроз змушує країни вступати у тісну міжнародну взаємодію. Співпраця на європейському рівні потрібна не лише для ефективної підготовки до кібератак, а й для своєчасної реакції на них. Комплексна державна стратегія кібербезпеки – перший крок на цьому шляху, вважають у європейських країнах.

16 грудня 2020 року Комісія та Верховний представник ЄС із закордонних справ та безпекової політики представили нову Стратегію кібербезпеки ЄС, яка є ключовим компонентом проєкту з формування цифрового майбутнього Європи, Плану відновлення для Європи та Стратегії для Союзу безпеки ЄС (*New EU*, 2021). Стратегія кібербезпеки підвищить колективну стійкість Європи до кіберзагроз і зробить свій внесок у забезпечення можливості для всіх громадян і підприємств повною мірою користуватися надійними електронними послугами та цифровими інструментами. Європейці, використовуючи під'єднані до мережі пристрої, електромережі, літаки, відвідуючи банки, державні адміністрації та лікарні, повинні мати гарантії своєї захищеності від кіберзагроз. Також нова Стратегія кібербезпеки сприяє зміцненню лідерства ЄС у галузі міжнародних норм і стандартів у кіберпросторі та покращенню співпраці з партнерами по всьому світу для просування глобального, відкритого, стабільного та безпечного кіберпростору, в основі якого лежить верховенство закону, права та основні свободи людини і демократичні цінності.

Перший закон про кібербезпеку в межах усього ЄС – Директива *NIS* (2016) – допоміг досягти загального високого рівня безпеки мереж та інформаційних систем у Євросоюзі. У зв'язку з входженням ЄС у цифрову епоху Закон про кібербезпеку (2019) надав Європі систему сертифікації продуктів, послуг та процесів із погляду кібербезпеки і посилив повноваження Агентства ЄС з кібербезпеки (*ENISA*).

Працюючи зі своїми партнерами на двосторонньому, регіональному та міжнародному рівнях, починаючи зі Стратегії кібербезпеки ЄС від 2013 року, ЄС веде послідовну та цілісну політику в галузі кібербезпеки, а саме підтримує треті країни у підвищенні їх кіберстійкості, використавши інструменти кібердипломатії ЄС (від 2017) та вперше застосувавши режим кіберсанкцій 2019 року (поширивши їх на 8 фізичних осіб та 4 юридичні особи та організації) (*Мужанова, 2024*). ЄС також значно просунувся у співпраці в галузі кібероборони, насамперед у контексті своєї Рамкової політики та Постійної структурованої співпраці (*PESCO*), а також у межах роботи Європейського оборонного агентства.

Пріоритетність кібербезпеки відображена у довгостроковому бюджеті ЄС на період 2021–2027 років, у межах програми «Цифрова Європа». Ця програма буде підтримувати дослідження в галузі кібербезпеки, розвивати інновації та інфраструктуру, кібероборону та галузь із забезпечення кібербезпеки. Крім того, у відповідь на кризу, пов'язану з війною в Україні, що викликала зростання кібератак, забезпечуються додаткові інвестиції в кібербезпеку відповідно до Плану відновлення для Європи (*Chiara, 2023*).

Нова Стратегія кібербезпеки ЄС захищає глобальний і відкритий Інтернет і одночасно гарантує не тільки забезпечення безпеки, а й захист європейських цінностей та основних прав кожної людини. Використовуючи досвід і досягнення останнього часу, вона пропонує конкретні заходи щодо нормативних, інвестиційних та політичних ініціатив ЄС.

ЄС підтримує розвиток нової Стратегії кібербезпеки безпрецедентною кількістю інвестицій у цифрові технології протягом наступних семи років (бюджет ЄС 2021–2027), зокрема в межах: Програми «Цифрова Європа», науково-дослідної ініціативи «Горизонти Європи» (*Horizon Europe*). Тому державам-членам рекомендується повною мірою використовувати Фонд відновлення і стійкості ЄС для підвищення кібербезпеки, в який ЄС державам-членам виділяє до 4,5 млрд євро сукупних інвестицій (у межах Центру компетенції в галузі кібербезпеки та Мережі координаційних центрів), більша частина яких має бути спрямована на малі та середні підприємства (*Chiara, 2023*).

Всі ці заходи націлені на посилення промислового та технологічного потенціалів ЄС у сфері кібербезпеки. ЄС має унікальну можливість об'єднати свої активи для підвищення стратегічної незалежності та просування свого лідерства в галузі кібербезпеки в цифровому ланцюжку поставок (включно з даними та хмарними обчисленнями, процесорними технологіями наступного покоління, надбезпечним зв'язком та мережами 6G, хоча ще в березні 2019 року Комісія у своїй Рекомендації говорила про кібербезпеку мереж покоління 5G) відповідно до цінностей та пріоритетів ЄС.

Французька Республіка виконує кіберзобов'язання в межах Ради Європи та Європейського Союзу. У 2001 році Франція підписала і в 2006 році ратифікувала Конвенцію щодо боротьби з кіберзлочинністю Ради Європи (відому як Будапештська конвенція) (*Convention, 2006*).

Норми Конвенції спрямовані на регулювання трьох основних блоків питань: зближення кримінально-правової оцінки злочинів у сфері комп'ютерної інформації; зближення національних кримінально-процесуальних заходів, спрямованих на збирання доказів під час розслідування таких злочинів; міжнародна співпраця в кримінально-процесуальній діяльності, спрямованій на збирання доказів скоєння таких злочинів.

Головна міжнародна ініціатива французької сторони у сфері інформаційно-комунікативних технологій – Паризький заклик до довіри та безпеки у кіберпросторі (листопад 2018 р.). У ньому були закріплені такі цілі:

- запобігати зловмисній кібердіяльності, яка загрожує окремим особам або критичним інфраструктурам або завдає їм значної невібіркової або системної шкоди, та усувати її;

– запобігати навмисним діям, які значно підривають доступність та цілісність центрального публічного ядра Інтернету;

– розвивати можливості щодо запобігання втручанню з боку іноземних суб'єктів задля дестабілізації виборчих процесів за допомогою зловмисної кібердіяльності;

– запобігати розкраданню інтелектуальної власності за допомогою інформаційно-комунікативних технологій, зокрема, промислових таємниць та іншої конфіденційної комерційної інформації для отримання конкурентних переваг для підприємств або для будь-якого комерційного сектору;

– розробляти засоби для запобігання поширенню шкідливих інструментів та комп'ютерних методів;

– посилити безпеку цифрових процесів, продуктів і послуг протягом усього терміну експлуатації та протягом усього ланцюжка постачання;

– підтримувати дії, спрямовані на розвиток сучасної комп'ютерної гігієни всіх учасників; вживати заходів, щоб перешкодити недержавним суб'єктам, зокрема з приватного сектору, вживати агресивні кібердії у відповідь на напад на них чи то для себе особисто, чи для інших недержавних суб'єктів;

– сприяти широкому ухваленню та впровадженню міжнародних норм відповідальної поведінки, а також заходів щодо посилення довіри в кіберпросторі (*La France, 2018*).

В останні роки Франція активізувала співпрацю з країнами-партнерами у сфері кібербезпеки. Наприклад, спільно із Сенегалом відкрила у 2018 році Національну регіональну спеціалізовану школу кібербезпеки у Дакарі. Цей проєкт спрямований на проведення короткострокових та адаптованих тренінгів для фахівців з кібербезпеки та високопоставлених державних службовців із Західної Африки (*Forum, 2018*).

Франція також доклала зусиль для ухвалення такого загальноєвропейського законодавства у кіберсфері, яке одночасно враховує вимоги конкурентоспроможності, специфіку цифрових технологій та міжнародні правозахисні гуманітарні стандарти (право на недоторканність приватного життя та захист персональних даних, захист критично важливої інфраструктури, боротьба з кібератаками, заборона терористичного контенту в Інтернеті).

Як приклади цього назвемо:

– Загальний Регламент захисту даних № 2016/679 (*GDPR*);

– Директиву з безпеки мереж та інформаційних систем № 2016/1148 (директива *NIS*);

– Регламент про *ENISA* (Агентство захисту даних), Європейського Союзу з кібербезпеки та сертифікації кібербезпеки інформаційних та комунікаційних технологій, який змінив Регламент про кібербезпеку № 526/2013 (*Regulation, 2019*).

У «Міжнародній стратегії Франції в галузі цифрових технологій» також наголошено на важливості продовження діалогу на основі співпраці з усіма зацікавленими приватними та державними суб'єктами, а також з усіма міжнародними партнерами, які готові до цього як на двосторонньому, так і на багатосторонньому рівнях. Зокрема, Франція брала активну участь в Організації економічної співпраці та розвитку. Вона працювала над організацією першого засідання Ради «Глобальний форум ОЕСР з цифрової безпеки з метою економічного та соціального процвітання»

у грудні 2018 року на тему «Відповідальність приватних суб'єктів за цифрову безпеку». Важливу увагу у межах цього напряму приділяли питанням конфіденційності, захисту даних та підвищення довіри до нових цифрових технологій, а також тому, як розвивати цифрову інфраструктуру за рахунок фінансування та ролі державного сектору.

Отже, у Французькій Республіці можна виділити такі основні механізми, що забезпечують кібербезпеку:

- розробка єдиної стратегії кібербезпеки;
- визначення законодавчої бази для забезпечення кібербезпеки та боротьби з кіберзлочинністю;
- впровадження процедур співпраці з приватним сектором, особливо з великими цифровими компаніями;
- визначення структури захисту критично важливої інфраструктури у кіберпросторі.

Узагальнюючи, можемо зазначити, що ці заходи виробляють кібервідповідальну поведінку будь-якої держави. Тому французькі національні правові механізми кібербезпеки можуть стати основою для формування спільних для всіх держав ООН стандартів та сприяти якісній міжнародній співпраці в кіберсфері.

Відмінною рисою німецького підходу до забезпечення кібербезпеки є його комплексний та фундаментальний характер, що передбачає цілу систему нормативних актів, планів та інститутів, покликаних реалізовувати ці плани. Ще у 2005 році у ФРН було розроблено та ухвалено Національний план захисту інформаційної інфраструктури, а у 2007 році – План реалізації захисту критичних елементів інфраструктури. Ці документи, розроблені за участю уряду, бізнесу та інших структур, визначають загальну стратегію реагування на кризи у сфері інформаційних технологій та містять рекомендації бізнес-спільноті щодо дій у разі великих кібератак. Згідно з цими документами оператори розробляють і повинні застосовувати відповідні процедури раннього оповіщення, причому в документах чітко визначено структури та особи, яких інформують насамперед після виявлення та фіксації тієї чи іншої кризової ситуації. Крім того, у Плані реалізації захисту критичних елементів інфраструктури містяться вказівки щодо створення робочих груп із різних аспектів кібербезпеки, включно з кризовим управлінням, проведенням антикризових навчань, забезпеченням постійної доступності критично важливих сервісів.

Створене в 1991 році Федеральне управління з інформаційної безпеки Німеччини (*BSI*), яке є складовою МВС, є головним органом, відповідальним за національну кібербезпеку ФРН. Цей орган формує політику та план дій у галузі інформаційної безпеки для запобігання, визначення та реагування на інциденти і кризи у цій сфері. Федеральне управління з інформаційної безпеки Німеччини, зокрема, формує попередження та оповіщення про віруси й інші шкідливі програми в ІТ-продуктах та послугах, дає рекомендації щодо протидії шкідливим програмам та діям, а також організує інформаційний обмін із більш ніж 50 000 недержавних організацій, включно з малим та середнім бізнесом.

У 2011 році у ФРН було ухвалено нову Федеральну стратегію кібербезпеки, яка покликана забезпечити багатосторонній міжвідомчий підхід до безпеки в

кіберпросторі на національному рівні. Стратегія орієнтована передусім на захист критично важливих інформаційних структур та виявлення додаткових можливостей у сфері забезпечення безкризового функціонування інформаційної інфраструктури Німеччини (*Cyber, 2011*). Серед найважливіших напрямів стратегії можна назвати такі:

- безпека інформаційних технологій у Німеччині здійснюється на підставі спільної діяльності громадянського суспільства та держави, при цьому комплекс інструментів захисту від кіберзагроз постійно розширюється;

- за допомогою Національного центру кібербезпеки (*Nationales Cyber-Abwehrzentrum, NCAZ*) відбувається оптимізація оперативної співпраці між усіма органами державної влади та забезпечується захист від кібератак критично значущих об'єктів національної IT-інфраструктури та економіки;

- координація превентивних заходів і міждисциплінарних підходів у галузі кібербезпеки в державному та приватному секторах покладена на Національну раду кібербезпеки, яка є додатковою сполучною ланкою IT-управління на федеральному рівні за участю різних міністерств та інших федеральних органів;

- ефективний контроль за злочинністю в кіберпросторі містить цілий комплекс інститутів за участю підприємців і компетентних правоохоронних органів для розробки відповідних рекомендацій.

У квітні 2017 року збройні сили ФРН створили кіберкомандування (*Cyber and Information Space Command, CIS*), завданням якого є відбиття хакерських та шпигунських атак. Згідно з розробленим Бундесвером планом чисельність *CIS* становитиме 14,5 тис. співробітників, з яких 1,5 тис. будуть цивільними особами. Тож у ФРН налагоджено досить тісну взаємодію цивільних і військових структур у галузі кіберзахисту та відбиття хакерських і шпигунських атак у кіберпросторі.

Слід ще раз наголосити, що система заходів та інститутів у Німеччині постійно розвивається залежно від посилення старих або виникнення нових кіберзагроз. Так, уряд розглядав питання про можливе внесення змін до конституції країни для завдання ударів по хакерах, що атакують приватні комп'ютерні мережі. Під заходами протидії хакерам розуміється, зокрема, відключення серверів, які використовують під час здійснення кібератак. Крім того, це вказує на рішучість ФРН будь-якими засобами захистити свою інформаційну інфраструктуру від численних кіберзагроз, не зупиняючись навіть перед зміною основного закону країни – конституції.

Італійський досвід організації кібербезпеки полягає у використанні американської моделі кіберкомандування. Він був нормативно закріплений у «Білій книзі з оборони» у 2015 році.

Організоване два роки по тому об'єднане командування кібернетичних операцій було спрямоване на поетапне досягнення повної оперативної готовності протистояти кіберзагрозам та кібервійнам, реалізованим через комп'ютерні мережі, та реагування на них.

Діяльність зазначеного підрозділу проводять у сфері кіберзахисту та захисту кібермереж. У першому випадку реалізують статичну та динамічну безпеку цілісності мережі та доступності інформації спільно з іншими підрозділами і структурами військового відомства. Друга пов'язана з проведенням експертизи та оцінки вразливості кібермережі, забезпечення швидкого й адекватного втручання для

запобігання настанню негативних наслідків та вирішення кіберінцидентів, які виникли. З цією метою також передбачено спеціальне діагностичне тестування систем на захищеність від несанкціонованого проникнення.

Об'єднане командування кібернетичних операцій Італії підпорядковане начальнику штабу оборони збройних сил та містить такі важливі командно-штабні елементи, як відділ персоналу, експериментальний оперативний підрозділ, який збирає інформацію про потенційних кіберзлочинців і кіберзагрози, розробляє та планує заходи протидії загрозам та кібератакам, а також кіберфілія спеціалізованої освітньої організації

Така важлива структура кібербезпеки Італійської Республіки, як Об'єднане командування кібернетичних операцій, забезпечує підтримку на високому організаційно-методичному та технічному рівнях проведення військових операцій, планує і проводить наступальні операції та виступає координуючим органом між італійськими збройними силами й іншими організаціями та спільнотами кібербезпеки (*Defending, 2017*).

Здійснює внутрішньодержавну кібербезпеку Департамент інформаційної безпеки, один із заступників директора якого безпосередньо відповідальний за цей напрям діяльності. Він координує діяльність Об'єданого командування кібернетичних операцій та державної поліції, центру захисту критично важливих об'єктів від злочинів проти інформатики, а також національний центр інформаційної безпеки, з яким через спеціально організовані кібермережі та кіберінфраструктури взаємодіють інші федеральні міністерства та департаменти Італії.

За підсумками дослідження можна дійти висновку, що з урахуванням взаємодії національних і наднаціональних органів ЄС політика забезпечення кібербезпеки стикається з цілою низкою проблем та труднощів. Незважаючи на безліч законодавчих та інших актів ЄС у галузі кібербезпеки, а також на створення різних національних і наднаціональних органів, система заходів щодо забезпечення кібербезпеки недостатньо сформована та недостатньо ефективна. Одна з основних причин полягає в тому, що керівництво низки європейських держав лише за останні роки вирішило реалізувати єдину політику у сфері кібербезпеки. Крім цього, важливою обставиною, що заважає проведенню єдиної узгодженої політики, є те, що члени ЄС суттєво відрізняються за економічними, технічними та інформаційними можливостями. Тому одні країни ЄС (як, наприклад, Німеччина, Франція чи Італія) більш розвинені у сфері кібербезпеки та кіберзахисту, ніж інші (наприклад, Греція чи Латвія). Система заходів у сфері кібербезпеки на національному та наднаціональному рівнях інтенсивно розвивається, але при цьому стикається з численними труднощами відповідно до рішень та вироблення єдиної політики забезпечення кібербезпеки. Очевидно, що ця політика потребує подальшого вдосконалення. Тим не менш, досвід забезпечення кібербезпеки в країнах ЄС може бути дуже корисним для України щодо розробки нормативних актів та підходів до узгодження заходів із забезпечення кібербезпеки на міжрегіональному та міждержавному рівнях.

3. Система забезпечення кібербезпеки в країнах Азії.

Погляди Китаю на інформаційне протиборство формуються переважно під впливом американських концепцій інформаційних операцій. Однак на відміну від США, що прагнуть до глобального домінування, китайська концепція є оборонною і

її головним завданням є протидія передбачуваній військовій загрозі з боку Сполучених Штатів.

Залежно від масштабу, характеру розв'язуваних завдань, використовуваних сил і засобів у Китаї розрізняють два види інформаційного протиборства (*Шевченко, 2022*):

1) у широкому сенсі – дії, що виконують на державному рівні у всіх сферах, потай або явно як у мирний, так і у воєнний час. Це передбачає встановлення контролю над інформаційним простором країн, які становлять загрозу національним інтересам КНР, а також для забезпечення власної інформаційної безпеки;

2) у вузькому значенні – здійснюються безпосередньо під час воєн і збройних конфліктів і обмежені просторовими рамками театрів воєнних дій.

На думку фахівців Генерального штабу Національно-визвольної армії Китаю, основними заходами щодо інформаційного протиборства, зокрема, слід вважати:

- керований інформаційний вплив (поширення або доведення до противника хибної чи спотвореної інформації);

- програмно-апаратний вплив через застосування інформаційної зброї на високотехнологічні системи ураження та автоматизовані системи управління військами, що розгортаються на базі мережевої телекомунікаційної інфраструктури;

- захист від інформаційного впливу супротивника;

- розвідувально-аналітичне забезпечення, що полягає у виявленні найважливіших об'єктів інформаційної інфраструктури противника, оцінці їх доступності, визначенні основних способів та тривалості впливу на них; оцінці та прогнозуванні загроз інформаційній безпеці; аналізі результатів проведених заходів інформаційного протиборства та у наданні командуванню потрібних даних для ухвалення рішень.

На думку китайського керівництва, у сфері розвитку інформаційно-комунікативних технологій країна поки що відстає від найбільш розвинених у військовому та економічному відношенні країн, що говорить про її неготовність нині до ведення інформаційної війни і досягнення інформаційної переваги. Тому планують прискорити комплексний розвиток усіх компонентів інформаційного протиборства, насамперед у військовій галузі. Це стосується, зокрема, розвитку інформаційної інфраструктури та технологій військового призначення, а також спеціальної підготовки особового складу.

Визнаючи своє відставання від провідних країн світу у сфері створення цифрових систем з урахуванням сучасних інформаційно-комунікативних технологій, КНР робить ставку на формування можливостей щодо нестандартних інформаційних атак та інших асиметричних дій.

Багато в чому політика кібербезпеки Китаю побудована на повному заміщенні власними інформаційними продуктами іноземних продуктів. На території КНР заборонені усі закордонні месенджери. У січні 2011 року розробник *Tencent* представив власний месенджер *Weinix* та його глобальну версію *WeChat* (*WeChat, 2024*). Сервіс об'єднує у собі обмін миттєвими повідомленнями, соціальну мережу, мобільні платежі, купівлі авіаквитків та ін.

Версія, яка працює на території материкового Китаю, підпорядковується політиці конфіденційності *Weinix*, що передбачає фільтрацію контенту, який ставить

під загрозу національну безпеку, розголошує державні таємниці чи підриває державну владу та національну єдність. Китайський уряд може отримати доступ до логів, текстових повідомлень та розташування своїх користувачів для забезпечення державної безпеки (*WeChat*, 2024).

Аналогічна ситуація і з застосунком *TikTok*. Локальна версія під назвою «Доуїнь» підпорядковується вимогам державної безпеки та цензурним обмеженням. Між собою версії не пов'язані, але мають однакові функціонал та можливості.

Важлива відмінність китайської парадигми кібербезпеки – це відкритість. Уряд відкрито каже, що блокування відбуваються заради державної безпеки. На законодавчому рівні прописані обмеження до публікацій, наприклад, заборона цитування та посилання на іноземні джерела у ЗМІ без схвалення.

Також для китайського підходу до безпеки інформаційного простору характерні:

- заміщення іноземних ресурсів місцевими;
- розмежування застосунків на локальну та глобальну версії;
- популяризація власних майданчиків;
- спадкоємність та поліпшення іноземних майданчиків.

Стратегію кібербезпеки Японії можна розбити на кілька ключових галузей:

- посилення політик, спрямованих на боротьбу з можливими масовими кібератаками, та заснування органу, відповідального за запобігання атакам;
- запровадження політик, що легко адаптуються до змін у сфері інформаційної безпеки;

- перевага активних політик інформаційної безпеки над пасивними.

Основні заходи, описані у стратегії Японії, передбачають:

- управління ІТ-ризиками для безпечного життя суспільства;
- запровадження політики, яка посилить державну безпеку, покращить управління кризами в кіберпросторі і не суперечитиме політиці використання інформаційно-комунікаційних систем, яка є основою для соціоекономічної діяльності;

- запровадження тривекторної політики, що комплексно зачіпає проблеми національної безпеки, управління кризами та захист суспільства/особи. Особливо важливою є політика інформаційної безпеки суспільства/особи;

- запровадження політики інформаційної безпеки, яка б не суперечила стратегії економічного зростання;

- участь та розвиток міжнародних альянсів.

У квітні 2005 року в Японії був заснований Національний центр інформаційної безпеки (*National Information Security Center, NISC*), основним завданням якого стала координація впровадження першої національної стратегії інформаційної безпеки та посилення захисту інформаційного простору. У травні того ж року було створено Раду з питань політики інформаційної безпеки (*Information Security Policy Council, ISPC*), яка у лютому 2006 року представила Першу національну стратегію з питань інформаційної безпеки. Документ визначав стратегічний підхід до захисту інформації та передбачав розробку комплексного плану на три роки (*Gady*, 2017).

Завдання *NISC* містили надання державним установам потрібної інформації, встановлення партнерських відносин із приватним сектором для обміну передовим

досвідом, а також розвиток міжнародної співпраці в галузі інформаційної безпеки. При цьому кібербезпеку розглядали переважно з технічної точки зору, а основний акцент робився на ролі інформаційних технологій у японському суспільстві та їх впливі на економічний розвиток. Політичного значення питання кібербезпеки майже не набуло.

У результаті координація та реалізація політики інформаційної безпеки, а також заходів із протидії кіберзагрозам, були розподілені між чотирма основними установами: Національним агентством поліції (*NPA*), Міністерством внутрішніх справ та зв'язку (*MIAC*), Міністерством економіки, торгівлі та промисловості (*METI*) та Міністерством оборони Японії (*JMOD*). Водночас кожне з цих міністерств діяло відповідно до власної стратегії у сфері кібербезпеки (*Gady, 2017*).

ISPC уперше представив Стратегію кібербезпеки у червні 2013 року, використовуючи термін «кібер» замість «інформація», як це було у попередніх стратегічних документах. Це свідчило про розширення підходу до протидії загрозам у кіберпросторі. Нова урядова політика, викладена у документі, ставила за мету формування «нації з питань кібербезпеки», оскільки кібератаки почали сприймати як питання національної безпеки та кризового управління. Таке трактування засвідчило важливу зміну у ставленні до кіберзагроз (*Моренчук, 2020*).

Вперше у стратегічному документі було чітко окреслено роль Міністерства оборони у кіберзахисті, особливо у випадках атаки на національному рівні, в яких могли бути задіяні іноземні уряди. Стратегія, ймовірно, натхненна американськими підходами, визначала кіберпростір як новий театр ведення бойових дій. У документі йшлося про потребу у зміцненні кіберзахисного потенціалу Сил самооборони Японії (*JSDF*), зокрема через створення спеціального підрозділу кіберзахисту. Також порушували питання чіткого розподілу відповідальності між Міністерством оборони (*JMOD*) та цивільними відомствами у сфері захисту критичної інфраструктури та оборонних систем, що свідчило про тенденцію до мілітаризації японської кібербезпеки (*Моренчук, 2020*).

Стратегія наголошувала на важливості партнерства між державним і приватним секторами, зокрема через створення «системи обміну інформацією, заснованої на угоді про конфіденційність». Крім того, передбачалося посилення Координаційної групи урядових операційних служб безпеки, Групи реагування на комп'ютерні загрози та Координаційного центру з питань кібербезпеки. Документ також представив найбільш комплексний підхід Японії до кібердипломатії. Поряд із наголосом на міжнародну співпрацю та діалог з країнами-однодумцями, стратегія окреслила зусилля країни у формуванні глобальних норм поведінки в кіберпросторі. Особливу увагу приділяли американсько-японському альянсу як ключовому чиннику у розробці цих норм, а також підтримці багатостороннього підходу до управління Інтернетом (*Моренчук, 2020*).

Отже, у Японії створені інституційні й організаційні механізми формування та забезпечення кібербезпеки, які постійно удосконалюють. Розроблені нормативно-правові документи, що регламентують діяльність спеціально створених інституцій із кібербезпеки та основні засади забезпечення кібербезпеки в Японії.

Проаналізуємо основні положення формування та розвитку кібербезпеки в Таїланді.

У 2017 році була опублікована Національна стратегія кібербезпеки Таїланду на 2017–2021 роки (*National Cybersecurity Strategy 2017–2021*) (*National Cybersecurity Strategy, 2017*), яка розрахована на застосування протягом чотирьох років. Це перше керівництво з національної політики Таїланду у сфері кібербезпеки, яке поставило за мету підвищення ролі держави у боротьбі з кіберзагрозами, посилення потенціалу в цій галузі, вдосконалення центрального механізму управління національною кібербезпекою, а також захист інфраструктури, підвищення поінформованості у всіх секторах та зміцнення співпраці з іншими країнами.

Досягнення мети Національної стратегії кібербезпеки на 2017–2021 роки можливе через вирішення дев'яти завдань: 1) підвищення довіри у кожному секторі до реалізації усіх форм кібердіяльності; 2) захист інформаційної інфраструктури, яка керує інформаційними системами, та розвиток можливості для боротьби з кіберзагрозами; 3) захист національних інтересів та національної безпеки від старих та нових загроз; 4) зміцнення цифрової економіки; 5) підвищення інтеграції та співпраці, включно з обміном інформацією про кібербезпеку між інституційними елементами системи інформаційної безпеки; 6) розвиток потенціалу агентств та збільшення можливостей працівників у сфері кібербезпеки; 7) просування культури відповідального використання кіберпростору; 8) сприяння роботі із запобігання та припинення злочинності; 9) підвищення міжнародної ролі Таїланду у підтримці безпеки (*National Cybersecurity Strategy, 2017*).

Цей документ супроводжується двома додатками у формі таблиць. Перша таблиця показує взаємозв'язки національних місій, політик, стратегій та генеральних планів із Національною стратегією кібербезпеки на 2017–2021 роки, друга розкриває докладний оперативний план її реалізації за кожним із напрямів: 1) стимулювання всіх секторів до різних видів кіберактивності; 2) захист критично важливої інформаційної інфраструктури та розробка потенційних відповідей на кіберзагрози; 3) захист національних інтересів від нових та старих кіберзагроз; 4) зміцнення цифрової економіки; 5) підвищення обізнаності та просування внутрішньої співпраці під час забезпечення кібербезпеки; 6) заохочення культури правильного використання кіберпростору; 7) сприяння роботі з профілактики та боротьби зі злочинністю; 8) просування ініціатив Таїланду у сфері кібербезпеки на регіональному та міжнародному рівнях.

28 травня 2019 року набув чинності Закон про кібербезпеку Таїланду 2019 року (*Cybersecurity Act, 2019*), який ухвалили для управління, сприяння та реагування на цифрову економіку держави, що швидко зростає. Він регулює нагляд за діяльністю в галузі кібербезпеки, а також запобігання і боротьбу з «кіберзагрозами», які в широкому сенсі визначаються як будь-які дії або незаконні дії з використанням комп'ютера, комп'ютерної системи або небажаної програми з наміром заподіяти шкоду будь-кому, комп'ютерній системі, комп'ютерним даним або іншим відповідним даним, а також безпосередні загрози, які можуть пошкодити або вплинути на роботу комп'ютера, комп'ютерної системи або інших відповідних даних (*Cybersecurity Act, 2019*).

Однією з особливостей цього закону є вказівка у преамбулі тези про обмеження прав і свобод людини, гарантованих Конституцією Королівства Таїланд, задля ефективного захисту кібербезпеки та розроблення підходів для захисту, подолання та

зниження ризику кіберзагроз, що впливають на національну безпеку і громадський порядок. Ухвалення цього закону відповідає критеріям, установленим у статті 26 Конституції Королівства Таїланд (*Cybersecurity Act, 2019*).

Закон складається із чотирьох розділів (*chapters*). Розділ 1 регламентує правовий статус Комітету (*Committee*), що складається з Національного комітету кібербезпеки (*National Cybersecurity Committee, NCSC*) і Комітету з регулювання кібербезпеки (*Cybersecurity Regulating Committee*). Розділ 2 присвячений регулюванню діяльності Адміністрації Національного комітету кібербезпеки (*Office of the National Cybersecurity Committee*). Розділ 3 – системі підтримки кібербезпеки (*Maintaining Cybersecurity*), що включає політики та плани (*policies and plans*), управління (*management*), критичну інформаційну інфраструктуру (*critical information infrastructure*) та протидію кіберзагрозам (*coping with cyberthreats*). Останній розділ містить положення про покарання (*penalty provisions*).

У зазначеному законі передбачено, що «підтримка кібербезпеки» означає будь-яку міру або процедуру, встановлену для запобігання, подолання та зниження ризику кіберзагроз як усередині країни, так і за її межами, які впливають на національну, економічну, військову безпеку та громадський порядок. «Інцидент кібербезпеки» означає інцидент, викликаний будь-якою дією або незаконним обов'язком, вчиненим через комп'ютер або комп'ютерну систему, який може пошкодити або вплинути на безпеку в цілому комп'ютера, комп'ютерних даних, комп'ютерної системи або інших даних, пов'язаних із комп'ютерною системою.

«Рішення кібербезпеки» означає акт вирішення проблеми кібербезпеки з використанням персоналу, процесів і технологій через комп'ютер, комп'ютерну систему, комп'ютерну програму або будь-яку послугу, що стосується комп'ютера, для створення впевненості та підвищення кібербезпеки комп'ютера, комп'ютерної даних, комп'ютерної системи або інших (*Cybersecurity Act, 2019*).

Цікавим є визначення термінів, що мають відношення до критичної інформаційної інфраструктури – ключового об'єкта кібербезпеки. Тайський закон визначає її як комп'ютер або комп'ютерну систему, яку урядове агентство або приватна організація використовують у своїх операціях, пов'язаних із підтримкою національної, суспільної, національної економічної безпеки чи інфраструктури у суспільних інтересах. Зазначимо, що закон оперує терміном «організація критично важливої інформаційної інфраструктури», якою можуть бути урядове агентство або приватна організація, відповідальна за надання послуг критичної інформаційної інфраструктури або яка безпосередньо надає ці послуги. Контроль та регулювання діяльності організації критичної інформаційної інфраструктури здійснюють «наглядова чи регулююча організація», тобто урядове агентство, приватна організація або особа, яка уповноважена законом.

Національний комітет кібербезпеки формується з таких посадових осіб: 1) прем'єр-міністр як голова; 2) директор з посади: міністр оборони, міністр цифрової економіки та суспільства, постійний секретар Міністерства фінансів, постійний секретар Міністерства юстиції, генеральний комісар Національного поліцейського управління та генеральний секретар Ради національної безпеки; 3) почесні директори в кількості не більше семи осіб, що їх призначає Кабінет міністрів з осіб, які мають знання, значний досвід у галузі кібербезпеки, інформаційних технологій та

комунікацій, захисту конфіденційності даних, науки, техніки, права, фінансів або інших відповідних аспектів (*Cybersecurity Act, 2019*).

Національний комітет кібербезпеки має такі обов'язки та повноваження: 1) пропонувати політику та план підтримки кібербезпеки; 2) визначати політику управління для підтримки кібербезпеки державних агенцій та організацій критичної інформаційної інфраструктури; 3) готувати оперативний план щодо підтримки кібербезпеки для розгляду Кабінетом міністрів; 4) встановлювати стандарти та методологію для поліпшення та розвитку систем обслуговування, що належать до підтримки кібербезпеки, встановлювати стандарти щодо комп'ютерної техніки, комп'ютерних систем, комп'ютерних програм, а також затверджувати стандарти сертифікації організацій критичної інформаційної інфраструктури, державних агенцій, наглядових чи регулюючих організацій, приватних організацій; 5) розробляти заходи та керівні засади для підвищення рівня знань і досвіду компетентних посадових осіб, включно з посадовими особами організації критичної інформаційної інфраструктури та іншими суб'єктами; 6) встановлювати межі співпраці з іншими національними та іноземними агентствами у сфері кібербезпеки; 7) відстежувати та оцінювати результати роботи відповідно до політики, загального та оперативного планів щодо підтримки кібербезпеки; 8) надавати висновки Комітету з цифрової економіки та суспільства або Кабінету міністрів з питань забезпечення кібербезпеки; 9) виступати із законодавчою ініціативою у сфері кібербезпеки тощо (*Cybersecurity Act, 2019*).

Комітет із регулювання кібербезпеки має такі обов'язки та повноваження: 1) контроль за виконанням плану з підтримки кібербезпеки; 2) відстеження та вжиття заходів для протидії кіберзагрозам на критичному рівні; 3) регулювання діяльності національних координуючих агентств із безпеки комп'ютерних систем, реагування на інциденти та комп'ютерної криміналістики; 4) регулювання діяльності організації критичної інформаційної інфраструктури; 5) моніторинг рівня кіберзагроз, включно з докладною інформацією про заходи щодо запобігання, протидії, оцінки на кожному рівні з подальшим поданням звіту Національному комітету кібербезпеки.

При розробленні стандартів діяльності організацій критичної інформаційної інфраструктури повинні бути розглянуті принципи управління ризиками, що містять щонайменше такі підходи та заходи: опис ризику, який може виникнути щодо комп'ютера, комп'ютерних даних, комп'ютерної системи, іншої інформації, пов'язаної з комп'ютерною системою, майном, життям та здоров'ям людини; заходи із запобігання ризику; заходи з вивчення та моніторингу кіберзагроз; заходи реагування для виявлення кіберзагроз; заходи щодо усунення та відновлення збитків, завданих кіберзагрозою.

Важливим аспектом забезпечення кібербезпеки у Таїланді є протидія кіберзагрозам. Як зазначалося вище, Комітет з регулювання кібербезпеки уповноважений визначати три рівні кіберзагроз: 1) несерйозні кіберзагрози; 2) серйозні кіберзагрози; 3) критичні кіберзагрози. Характеристика кожного рівня загрози залежить від впливу такої загрози на державну інфраструктуру, національну безпеку, економіку, громадську охорону здоров'я та суспільство. Вжиті заходи визначаються рівнем небезпеки: у разі серйозної кіберзагрози уповноважені органи мають право перевіряти комп'ютери, комп'ютерні системи та кібердані, а також

вилучати комп'ютери, комп'ютерні системи або будь-яке інше обладнання (*Cybersecurity Act, 2019*).

Отже, заходи щодо забезпечення кібербезпеки у Таїланді встановлює відповідний Закон. Закон про кібербезпеку регулює ефективний механізм забезпечення інформаційної безпеки в кіберпросторі як в інституційному, так і в нормативно-правовому аспекті. У першому випадку створено вертикаль державного управління та моніторингу, у другому – визначено сектори критичної інформаційної інфраструктури та мінімальні вимоги до організацій такої інфраструктури. Відмінними рисами аналізованого закону є нормативне обґрунтування обмеження права і свободи людини під час реалізації його положень, і навіть встановлення кримінальних санкцій за скоєння злочинів посадовими особами як державних органів, так і приватних компаній. Такі санкції виступають як додаткова гарантія прав і свобод людини у сфері інформації та персональних даних.

Висновки. В останнє десятиліття глобальний інформаційний простір дедалі більше перетворюється на арену міждержавного суперництва, боротьби за досягнення стратегічних і тактичних політичних цілей. У 2011 році опубліковано стратегії кібербезпеки низки найбільших держав світу (США, Франції, ФРН та ін.), в яких проголошено курс цих країн на будівництво кіберзбройних сил. Американські військові доктринально закріпили за кіберпростором статус п'ятого театру військових дій (поряд із сушею, водою, повітрям та космосом). Більшість європейських країн, особливо як входять до блоку НАТО, також розробили свої стратегії кібербезпеки, хоча здебільшого вони є деяким перекладом доктринальних документів своїх партнерів.

Свій стратегічний погляд на вирішення проблем кібербезпеки мають Китай, Японія, Таїланд, зокрема, щодо формування інституційного та організаційного забезпечення кібербезпеки у країні та світі.

Водночас у більшості національних стратегій кібербезпеки, блокових доктринах країн західного світу слабо виражене занепокоєння міжнародного співтовариства в питаннях недопущення чергового витка гонки озброєнь на якісно новому рівні розвитку інформаційно-комунікативних технологій, зниження небезпеки загрози агресивного використання цих технологій для силового вирішення злочинних діянь у глобальному інформаційному просторі.

Тому сьогодні головне питання, яке постає перед світовою спільнотою, полягає в такому: як зберегти весь позитивний потенціал глобального інформаційного простору і водночас нейтралізувати негативні та деструктивні тенденції його використання?

Одним із першочергових кроків на шляху до вирішення цього питання має стати розроблення та ухвалення на рівні Організації Об'єднаних Націй документа, що закріплює фундаментальні засади діяльності у глобальному інформаційному просторі та забезпечення безпеки цієї діяльності.

References:

- Моренчук А.А., Моренчук А. А. Сфера кібербезпеки у сучасній Японії. URL: <https://surl.li/pyesyx>
- Мужанова Т., Легомінова С., Щавінський Ю., Якименко Ю., Нестеренко Г. Основні підходи й напрями розвитку політики кібербезпеки Європейського Союзу. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2024. № 4(24). С. 133–149. URL: <https://doi.org/10.28925/2663-4023.2024.24.133149>.

- Погоріла Н. Концептуальний вимір зовнішньої політики США на початку XXI ст. *Вісник Київського національного університету імені Тараса Шевченка. Міжнародні відносини*. 2016. Вип. 1. С. 33-36. URL: http://nbuv.gov.ua/UJRN/VKNU_mv_2016_1_8
- Скорик А.Б., Ярош С.П. Еволюційний розвиток концепції мережево-центричних війн, системно-концептуальні основи теорії дата-центричних операцій. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2020. № 4(66). С. 26–34. URL: <https://doi.org/10.30748/zhups.2020.66.03>.
- Стежко С.М., Шевченко Т.О. Сучасний досвід США у сфері забезпечення кібербезпеки. *Інформація і право*. 2021. № 2(37). С. 139–144. URL: <http://il.ippi.org.ua/article/view/238349>
- Шевченко Ю.Г. Національна політика кібербезпеки Китаю: інституціональний тиск. *Китаєзнавчі дослідження*. 2022. № 1. С. 5–21. URL: <https://doi.org/10.51198/chinesest2022.01.005>
- Biden-Harris Administration's National Security Strategy. URL: <https://surli.cc/vuhhql>
- Chiara P. G. Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review*. 2023. Vol. 53. <https://doi.org/10.1016/j.clsr.2024.105961>
- Convention on Cybercrime. URL: <https://rm.coe.int/1680081580>.
- Cyber coalition 2021 Concludes In Estonia. URL: <https://surli.cc/dsnbqz>
- Cyberpower and national security / Ed. by F.D. Kramer, S.H. Starr, L.K. Wentz. Washington, D.C.: National Defense University Press; Potomac Books, 2009. URL: <https://surl.li/ivzrge>
- Cybersecurity 2022 – USA. Global Practice Guides. URL: <https://surl.li/lczftb>
- Cybersecurity Act, B.E. 2562 (2019). Office of the Council of State. URL: <https://surl.li/wydkim>
- Cyber Security Strategy for Germany. URL: <https://surl.li/rkvjfi>
- Defending Italy Against Cyberattacks. URL: <https://surl.li/ztlxnz>
- Forum international de Dakar sur la paix et la sécurité en Afrique. URL: <https://dakarforum.org/>.
- Gady F.-S. Japan: The Reluctant Cyberpower. IFRI. Institut francais des relations internationales. URL: <https://surli.cc/ddaezq>
- La France et les Nations unies. URL: <https://surli.cc/rfwdbi>
- Military perspectives on cyberpower / Ed. by L.K. Wentz, Ch.L. Darry, S.H. Starr. Washington, D.C.: Center for Technology and National Security Policy at National Defense University, 2009. URL: <https://surl.li/cwvwlw>
- National Cyber Strategy of the United States of America. (2018). (n.d.). www.whitehouse.gov. URL: <https://surl.li/kkrutg>
- National Cybersecurity Strategy 2017-2021. Council of Europe. URL: <https://surl.li/ohxhpm>
- National Plan to Combat Cybercrime 2022. URL: <https://surl.li/jwjyhg>
- New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. Press release. December 16, 2020. URL: <https://surl.li/vduuka>
- Remarks by National Security Advisor Jake Sullivan on the Biden-Harris Administration's National Security Strategy. URL: <https://surli.cc/zvingo>
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (In force) URL: <https://surli.cc/iuivsu>

CHAPTER 5. INNOVATIONS IN OCCUPATIONAL HEALTH AND SAFETY

Yuliana BILASH

Candidate of Science/Hons. Science, Associate Professor of the Department of Labor Protection and Technological Equipment in Animal Husbandry, Lviv National University of Veterinary Medicine and Biotechnology named after S.Z. Gzhytsky
(Pekarska, 50, Lviv, Ukraine)

ulianabilach@gmail.com

<https://orcid.org/0000-0002-8890-667X>

Abstract. Innovation in occupational safety is a key direction of development in the modern working environment. In a world where technology is rapidly changing all aspects of our lives, occupational safety is also undergoing transformations aimed at ensuring safe and comfortable working conditions for every employee. The use of modern tools, such as sensors for monitoring equipment status, mobile applications for risk assessment, and robotic systems for performing dangerous operations, allows us to significantly reduce the human factor in the occurrence of emergency situations. The use of modern tools, such as sensors for monitoring equipment status, mobile applications for risk assessment, and robotic systems for performing dangerous operations, allows us to significantly reduce the human factor in the occurrence of emergency situations.

Keywords: occupational safety, innovation, digital technologies, automation, virtual reality, Internet of Things (IoT), risk management, artificial intelligence.

Introduction. In today's digitalization and technological progress, innovations in occupational safety are becoming an integral part of the sustainable development of enterprises. The introduction of intelligent data analysis systems allows you to predict potential risks and quickly respond to changes in the production environment. For example, artificial intelligence technologies are able to analyze large amounts of data from sensors and warn about the possibility of equipment breakdowns or exceeding permissible parameters, which reduces the likelihood of accidents. An important component of innovations is employee training. Interactive simulators, virtual and augmented reality open up new opportunities for personnel training. Employees can master complex operations without risk to themselves, train safe behavior skills in crisis situations and better understand the consequences of ignoring safety rules.

The problem statement. Modern working conditions are characterized by the increasing complexity of production processes, the introduction of new technologies and increased risks to the health and safety of workers. Traditional approaches to occupational safety often prove to be insufficiently effective in preventing industrial injuries and occupational diseases. The use of innovative solutions, such as automated monitoring systems, artificial intelligence, the Internet of Things (IoT), augmented reality and new materials, opens up new opportunities for improving occupational safety. However, the widespread implementation of such technologies requires appropriate changes in the regulatory framework, significant financial investments. The relevance of research into

innovations in occupational safety is due to the development of effective mechanisms for introducing the latest technologies into production processes that reduce the number of accidents, increase work efficiency and ensure their lives.

Analysis of recent studies and publications. Recent studies and publications in the field of occupational health and safety indicate the active implementation of innovative approaches to improve worker safety and health. Here are some key areas of innovation: 1. Use of digital technologies: Development and implementation of mobile applications for monitoring working conditions, virtual and augmented reality for employee training, as well as an Internet of Things (IoT) system for monitoring safety in the workplace.

In the field of public administration and administration, the problems of public administration of labor protection in Ukraine are investigated. It is emphasized that public administration of labor protection is being actualized today in connection with the constitutional proclamation of the life and health of a person as the highest social value in the state. The methodology of scientific research is based on the methods and means of public administration, which are highlighted through the prism of the Law of Ukraine “On Labor Protection”, which has a positive impact on public administration in this area, and at the same time it is taken into account that the specified legislative act was adopted when the basis of the economy was state, not private property, therefore the legal mechanisms of labor protection management in modern conditions were not fully involved. The scientific novelty of the results obtained is that the study substantiates that in connection with the transition of the state to market conditions, state supervision and control over labor protection, and legal mechanisms of liability for its violation, were weakened. (*Andrushko A.V. , 2023*)

The article examines the problems of occupational safety during war, which are an extremely important aspect of ensuring the safety and health of workers in the workplace. This study provides a general overview of the problem and consideration of various aspects of occupational safety in conditions of military conflict. The problems associated with the organization of safe work in conditions of war are analyzed, including ensuring fire safety, protection against explosions, the use of protective equipment, the implementation of safe procedures and compliance with labor protection norms and rules. The problems of psychological health of workers are also considered, including maintaining the emotional state and understanding military-psychological and stress factors. The current threats associated with armed conflicts are discussed, effective strategies are proposed to ensure the safety of workers and minimize the risks of emergencies. (*Buzhanska M.V. , 2024*)

ІННОВАЦІЇ В ОХОРОНІ ПРАЦІ

Інновації в охороні праці є ключовим напрямом розвитку сучасного виробничого середовища. У світі, де технології швидко змінюють усі аспекти нашого життя, охорона праці також зазнає трансформацій, спрямованих на забезпечення безпечних і комфортних умов роботи для кожного працівника. Використання новітніх технологій, таких як автоматизація, інтернет речей, штучний інтелект та інтерактивні навчальні платформи, дозволяє не лише зменшити ризики для здоров'я, але й створювати ефективніші системи контролю та управління безпекою. Такий підхід сприяє не лише збереженню життя та здоров'я працівників, але й підвищенню продуктивності, що є важливим чинником сталого розвитку будь-якої організації.

Інновації в охороні праці охоплюють широкий спектр технологічних, організаційних та методологічних змін, які спрямовані на запобігання нещасним випадкам, зменшення шкідливого впливу виробничих факторів та створення умов для сталого розвитку. Використання сучасних засобів, таких як сенсори для моніторингу стану обладнання, мобільні додатки для оцінки ризиків, роботизовані системи виконання небезпечних операцій, дозволяє суттєво знизити людський фактор у виникненні аварійних ситуацій. Крім того, значна увага приділяється психологічному та фізичному благополуччю працівників. Впровадження програм зниження стресу, регулярного медичного огляду, а також інтеграція практик добробуту в корпоративну культуру стають важливими елементами системи охорони праці. Усе це допомагає створити середовище, де працівники почуваються захищеними та мотивованими до продуктивної діяльності.

Інноваційні підходи також включають розробку нових стандартів і нормативів, які враховують сучасні виклики та специфіку різних галузей. Таким чином, інновації в охороні праці стають не лише засобом підвищення безпеки, а й важливим фактором, що впливає на конкурентоспроможність підприємств у глобальній економіці.

У сучасних умовах діджиталізації та технологічного прогресу інновації в охороні праці стають невід'ємною складовою сталого розвитку підприємств. Впровадження інтелектуальних систем аналізу даних дозволяє передбачати потенційні ризики та оперативно реагувати на зміни у виробничому середовищі. Наприклад, технології штучного інтелекту здатні аналізувати великі обсяги даних з сенсорів та попереджати про можливість поломок обладнання або перевищення допустимих параметрів, що знижує ймовірність аварій.

Важливою складовою інновацій є навчання працівників. Інтерактивні симулятори, віртуальна та доповнена реальність відкривають нові можливості для підготовки персоналу. Працівники можуть без ризику для себе освоювати складні операції, тренувати навички безпечної поведінки у кризових ситуаціях і краще розуміти наслідки нехтування правилами безпеки.

Крім того, інновації в охороні праці активно підтримують концепцію "зеленої економіки". Це включає використання екологічно чистих матеріалів, енергоефективних технологій і мінімізацію відходів виробництва. Такий підхід не лише зменшує вплив на довкілля, а й сприяє створенню здорових і комфортних умов роботи.

Взаємодія бізнесу, науки і держави також відіграє значну роль у розвитку інновацій в цій сфері. Державна підтримка, грантові програми та ініціативи, спрямовані на модернізацію підприємств, стимулюють впровадження новітніх технологій. Це, у свою чергу, сприяє створенню культури безпеки, де охорона праці є не лише формальністю, а й ключовою цінністю.

Інноваційні рішення стають гарантом не лише збереження здоров'я працівників, але й підвищення конкурентоспроможності компаній на глобальному ринку. Впровадження нових підходів дозволяє трансформувати охорону праці з обов'язкової вимоги в стратегічний інструмент, що приносить реальну користь і людям, і бізнесу.

Анотація. У статті розглядаються сучасні інноваційні підходи до охорони праці, спрямовані на підвищення рівня безпеки та зниження виробничого

травматизму. Проаналізовано впровадження цифрових технологій, штучного інтелекту, автоматизованих систем моніторингу та використання засобів індивідуального захисту нового покоління. Особлива увага приділяється концепціям «Нульового травматизму» (Vision Zero) та впровадженню стандартів Industry 4.0 в сферу охорони праці. Окреслено перспективи розвитку інноваційних рішень та їх вплив на ефективність системи безпеки праці.

У роботі розглянуто інноваційні рішення у сфері охорони праці, що сприяють створенню безпечного та комфортного робочого середовища. Досліджено роль цифрових технологій, Інтернету речей (IoT), доповненої реальності (AR), штучного інтелекту (AI) та біометричних систем у забезпеченні безпеки працівників. Описано сучасні методи управління ризиками, використання сенсорних пристроїв для моніторингу навколишнього середовища та персоналу, а також застосування автоматизованих систем аналізу небезпек. Визначено перспективи розвитку та вплив інноваційних технологій на ефективність охорони праці в умовах цифрової трансформації виробництва.

Ключові слова: охорона праці, інноваційні технології, цифровізація, штучний інтелект, Інтернет речей, управління ризиками, безпечне робоче середовище.

Сучасні умови праці характеризуються зростаючою складністю виробничих процесів, впровадженням нових технологій та підвищенням ризиків для здоров'я і безпеки працівників. Традиційні підходи до охорони праці часто виявляються недостатньо ефективними для запобігання виробничому травматизму та професійним захворюванням. Використання інноваційних рішень, таких як автоматизовані системи моніторингу, штучний інтелект, Інтернет-речей (IoT), доповнена реальність та новітні матеріали, відкриває нові можливості для підвищення безпеки праці. Однак широке впровадження таких технологій потребує відповідних змін у нормативно-правовій базі, значних фінансових інвестицій.

Актуальність дослідження інновацій в охороні праці зумовлена забезпеченістю розробки ефективних механізмів впровадження новітніх технологій у виробничі процеси, що зменшують кількість нещасних випадків, підвищують ефективність роботи та забезпечують їхнє життя.

Постановка проблеми. Сучасні умови праці характеризуються ускладненням виробничих процесів, впровадженням нових технологій та підвищенням ризиків для здоров'я та безпеки працівників. Традиційні підходи до охорони праці часто виявляються недостатньо ефективними для попередження виробничого травматизму та професійних захворювань. Використання інноваційних рішень, таких як автоматизовані системи моніторингу, штучний інтелект, Інтернет речей (IoT), доповнена реальність і нові матеріали, відкриває нові можливості для підвищення безпеки праці. Проте широке впровадження таких технологій потребує відповідних змін нормативно-правової бази, значних фінансових вкладень. Актуальність дослідження інновацій в охороні праці зумовлена розробкою ефективних механізмів впровадження у виробничі процеси новітніх технологій, що знижують кількість нещасних випадків, підвищують ефективність праці та забезпечують їх життя.

Аналіз останніх досліджень і публікацій. Останні дослідження та публікації в галузі гігієни та безпеки праці свідчать про активне впровадження інноваційних

підходів до підвищення безпеки та гігієни працівників. Ось деякі ключові сфери інновацій: 1. Використання цифрових технологій: розробка та впровадження мобільних додатків для моніторингу умов праці, віртуальної та доповненої реальності для навчання співробітників, а також системи Інтернету речей (IoT) для моніторингу безпеки на робочому місці.

У сфері державного управління та адміністрування досліджуються проблеми державного управління охороною праці в Україні. Наголошено, що державне управління охороною праці сьогодні актуалізується у зв'язку з конституційним проголошенням життя і здоров'я людини найвищою соціальною цінністю в державі. Методологія наукового дослідження базується на методах і засобах державного управління, які висвітлюються крізь призму Закону України «Про охорону праці», який позитивно впливає на державне управління в цій сфері, при цьому враховується, що зазначений законодавчий акт приймався, коли основою економіки була державна, а не приватна власність, тому правові механізми управління охороною праці в сучасних умовах були задіяні не повною мірою. Наукова новизна отриманих результатів полягає в тому, що в дослідженні обґрунтовано, що у зв'язку з переходом держави на ринкові умови послабилися державний нагляд і контроль за охороною праці та правові механізми відповідальності за її порушення. (Андрушко А.В., 2023)

У статті розглядаються проблеми охорони праці під час війни, які є надзвичайно важливим аспектом забезпечення безпеки та здоров'я працівників на виробництві. У даному дослідженні подано загальний огляд проблеми та розгляд різних аспектів охорони праці в умовах воєнного конфлікту. Проаналізовано проблеми, пов'язані з організацією безпечної праці в умовах воєнного часу, зокрема забезпечення пожежної безпеки, захисту від вибухів, використання засобів захисту, виконання безпечних процедур і дотримання норм і правил охорони праці. Також розглядаються проблеми психологічного здоров'я працівників, у тому числі збереження емоційного стану та розуміння військово-психологічних і стресових факторів. Обговорюються актуальні загрози, пов'язані зі збройними конфліктами, пропонуються ефективні стратегії забезпечення безпеки працівників та мінімізації ризиків виникнення надзвичайних ситуацій. (Бужанська М.В., 2024).

1. Цифрові технології в охороні праці

Інновації в охороні праці є ключовим напрямом розвитку сучасного виробничого середовища. У світі, де технології швидко змінюють усі аспекти нашого життя, охорона праці також зазнає трансформацій, спрямованих на забезпечення безпечних і комфортних умов роботи для кожного працівника. Використання новітніх технологій, таких як автоматизація, інтернет речей, штучний інтелект та інтерактивні навчальні платформи, дозволяє не лише зменшити ризики для здоров'я, але й створювати ефективніші системи контролю та управління безпекою. Такий підхід сприяє не лише збереженню життя та здоров'я працівників, але й підвищенню продуктивності, що є важливим чинником сталого розвитку будь-якої організації.

Інновації в охороні праці охоплюють широкий спектр технологічних, організаційних та методологічних змін, які спрямовані на запобігання нещасним випадкам, зменшення шкідливого впливу виробничих факторів та створення умов для сталого розвитку. Використання сучасних засобів, таких як сенсори для моніторингу стану обладнання, мобільні додатки для оцінки ризиків, роботизовані системи

виконання небезпечних операцій, дозволяє суттєво знизити людський фактор у виникненні аварійних ситуацій. Крім того, значна увага приділяється психологічному та фізичному благополуччю працівників. Впровадження програм зниження стресу, регулярного медичного огляду, а також інтеграція практик добробуту в корпоративну культуру стають важливими елементами системи охорони праці. Усе це допомагає створити середовище, де працівники почуваються захищеними та мотивованими до продуктивної діяльності.

Інноваційні підходи також включають розробку нових стандартів і нормативів, які враховують сучасні виклики та специфіку різних галузей. Таким чином, інновації в охороні праці стають не лише засобом підвищення безпеки, а й важливим фактором, що впливає на конкурентоспроможність підприємств у глобальній економіці.

У сучасних умовах діджиталізації та технологічного прогресу інновації в охороні праці стають невід'ємною складовою сталого розвитку підприємств. Впровадження інтелектуальних систем аналізу даних дозволяє передбачати потенційні ризики та оперативно реагувати на зміни у виробничому середовищі. Наприклад, технології штучного інтелекту здатні аналізувати великі обсяги даних з сенсорів та попереджати про можливість поломок обладнання або перевищення допустимих параметрів, що знижує ймовірність аварій.

Важливою складовою інновацій є навчання працівників. Інтерактивні симулятори, віртуальна та доповнена реальність відкривають нові можливості для підготовки персоналу. Працівники можуть без ризику для себе освоювати складні операції, тренувати навички безпечної поведінки у кризових ситуаціях і краще розуміти наслідки нехтування правилами безпеки.

Крім того, інновації в охороні праці активно підтримують концепцію «зеленої економіки». Це включає використання екологічно чистих матеріалів, енергоефективних технологій і мінімізацію відходів виробництва. Такий підхід не лише зменшує вплив на довкілля, а й сприяє створенню здорових і комфортних умов роботи.

Взаємодія бізнесу, науки і держави також відіграє значну роль у розвитку інновацій в цій сфері. Державна підтримка, грантові програми та ініціативи, спрямовані на модернізацію підприємств, стимулюють впровадження новітніх технологій. Це, у свою чергу, сприяє створенню культури безпеки, де охорона праці є не лише формальністю, а й ключовою цінністю.

Інноваційні рішення стають гарантом не лише збереження здоров'я працівників, але й підвищення конкурентоспроможності компаній на глобальному ринку. Впровадження нових підходів дозволяє трансформувати охорону праці з обов'язкової вимоги в стратегічний інструмент, що приносить реальну користь і людям, і бізнесу.

Цифрові технології стали потужним інструментом у трансформації підходів до забезпечення безпеки праці. Завдяки інтеграції сучасних інновацій, підприємства отримують змогу оперативно реагувати на потенційні загрози, зменшуючи ризики для здоров'я та життя працівників. Впровадження цифрових рішень підвищує ефективність процесів, забезпечує точність у контролі за умовами праці та сприяє створенню безпечного робочого середовища.

Цифрові технології відіграють важливу роль у сучасному розвитку охорони праці, покращуючи безпеку на робочих місцях та ефективність управління ризиками. Ось кілька основних напрямків їх застосування:

1. **Інтернет речей (ІоТ):** Використання сенсорних пристроїв для моніторингу здоров'я працівників та стану обладнання. Наприклад, датчики, що вимірюють температуру, вологість, рівень шуму або токсичні гази в робочому середовищі, дають змогу своєчасно реагувати на потенційні небезпеки.

2. **Біометричні технології:** Біометричні системи для контролю доступу, моніторингу стану здоров'я працівників (наприклад, аналіз серцевого ритму) дозволяють вчасно виявляти ознаки фізичного перенавантаження чи стресу.

3. **Доповнена реальність (AR):** AR-технології використовуються для навчання працівників, візуалізації ризиків та інструкцій по техніці безпеки в реальному часі, а також для проведення тренувань.

4. **Дистанційний моніторинг та управління:** Системи на основі даних з різних сенсорів дозволяють віддалено контролювати стан безпеки на виробництві, попереджати аварії, а також автоматизувати звітність і інші управлінські функції.

5. **Штучний інтелект (AI) і машинне навчання:** AI може аналізувати великі обсяги даних для виявлення патернів, що передбачають ризики або аварії, а також надавати рекомендації щодо поліпшення умов праці.

6. **Цифрові платформи для навчання та сертифікації:** Вебінари, онлайн-курси та інші платформи дозволяють працівникам проходити необхідні тренінги та отримувати сертифікати без необхідності присутності в класі.

7. **Віртуальна реальність (VR):** Використовується для створення симуляцій небезпечних ситуацій, що дозволяє працівникам тренуватися в умовах, які неможливо відтворити в реальному житті, без ризику для їхнього здоров'я.

Ці технології забезпечують високий рівень безпеки, ефективне навчання та швидку реакцію на можливі загрози, що важливо для підтримки здоров'я та безпеки працівників у будь-яких галузях.

Інтернет речей (ІоТ) — це концепція, яка передбачає інтеграцію різноманітних фізичних пристроїв з мережею Інтернет для збору, обробки та передачі даних. В охороні праці ІоТ технології можуть суттєво підвищити рівень безпеки, ефективності та запобігти нещасним випадкам на робочих місцях. Ось як саме це працює:

1. Сенсори для моніторингу умов навколишнього середовища

ІоТ-сенсори можуть бути встановлені в робочих приміщеннях для постійного моніторингу таких параметрів, як:

- **Температура та вологість:** Це особливо важливо на виробництвах, де кліматичні умови можуть впливати на безпеку працівників (наприклад, в умовах високих температур чи вологості може виникнути перегрів або ризик електричних замикань).

- **Рівень шуму:** Датчики, що вимірюють рівень шуму, можуть допомогти вчасно виявити небезпечні рівні звуку, які можуть призвести до втрати слуху чи стресу у працівників.

- **Концентрація токсичних газів:** Сенсори для виявлення газів, таких як монооксид вуглецю, аміак чи сірководень, можуть запобігти отруєнню працівників та вчасно активувати систему вентиляції або інші заходи безпеки.

- **Рівень пилу чи аерозолів:** У багатьох виробничих процесах можуть виникати шкідливі частинки, які негативно впливають на дихальну систему працівників.

2. Моніторинг стану обладнання. IoT-сенсори можуть також використовуватися для **моніторингу технічного стану обладнання**, що дає змогу запобігти поломкам або аваріям. Наприклад:

- **Вібраційні сенсори** можуть виявити аномальні рухи у машин, що можуть свідчити про майбутню поломку.
- **Температурні датчики** можуть попередити про перегрів обладнання, що часто призводить до пожеж або інших аварій.
- **Тиск і рівень масла** в механізмах можуть допомогти визначити, чи не знижено ефективність машини через технічні проблеми.

3. Моніторинг здоров'я працівників

Встановлення **персональних датчиків** на працівників дає змогу відстежувати їхнє фізичне стан. Це можуть бути пристрої, що вимірюють:

- **Частоту серцебиття та артеріальний тиск** — для виявлення стресу або перевтоми.
- **Температуру тіла** — що дозволяє виявити ранні ознаки перегріву або переохолодження.
- **Насичення крові киснем** (пульсоксиметрія) — що може бути корисно для працівників, які перебувають в умовах з нестабільним рівнем кисню.

4. Реакція на небезпеку та автоматичне реагування

Інтеграція IoT із системами автоматичного управління дозволяє:

- **Автоматично активувати вентиляцію** або **системи пожежогасіння** у разі виявлення високого рівня токсичних газів чи підвищеної температури.
- **Увімкнути аварійне освітлення** чи попередження для працівників, якщо рівень шуму або пилу перевищує допустимі норми.

5. Аналіз даних і попередження. Всі дані з сенсорів можуть бути зібрані на централізованій платформі, що використовує аналітику для:

- **Передбачення ризиків** і своєчасного попередження про потенційні небезпеки.
- **Ідентифікації небезпечних тенденцій** на підприємствах і надання рекомендацій щодо покращення умов праці.

Використання IoT у сфері охорони праці допомагає не тільки знизити кількість травм та аварій, а й підвищити загальний рівень безпеки на підприємстві завдяки постійному моніторингу та можливості швидкого реагування на будь-які зміни в умовах праці.

Біометричні технології набувають все більшого значення в охороні праці завдяки здатності забезпечити високий рівень безпеки та контролю за здоров'ям працівників. Вони використовують унікальні фізіологічні характеристики людини для автоматичної ідентифікації, моніторингу та оцінки стану здоров'я. Ось кілька основних напрямків застосування біометрії в охороні праці:

1. Контроль доступу. Біометричні системи контролю доступу використовуються для обмеження входу на небезпечні чи обмежені ділянки виробництва. Замість традиційних карток або PIN-кодів, біометричні методи пропонують більш надійний і точний спосіб ідентифікації, зокрема:

- **Розпізнавання відбитків пальців:** Це один з найбільш поширених способів ідентифікації, який забезпечує точну та швидку перевірку особи.

- **Розпізнавання обличчя:** Використовується в умовах, де важлива швидка ідентифікація без контакту, що є дуже корисним в умовах наявності спеціального захисного одягу.

- **Розпізнавання райдужної оболонки ока чи сітківки:** Ці методи забезпечують найвищий рівень точності та безпеки, оскільки райдужка ока є унікальною для кожної людини.

2. Моніторинг стану здоров'я працівників. Біометричні технології дають змогу здійснювати постійний моніторинг стану здоров'я працівників, що є важливим для запобігання нещасним випадкам, пов'язаним із фізичним перенавантаженням, стресом або іншими проблемами зі здоров'ям:

- **Аналіз серцевого ритму:** Використовуються біометричні пристрої для моніторингу частоти серцебиття працівників, що дозволяє вчасно виявити ознаки перевтоми, стресу або навіть серцево-судинних захворювань. При значних коливаннях або високих показниках серцевого ритму система може попередити про небезпеку і надати сигнал для відпочинку або медичного обстеження.

- **Вимірювання артеріального тиску:** Контроль за рівнем артеріального тиску дає можливість виявити ознаки гіпертонії чи інших серцево-судинних проблем, що можуть загрожувати здоров'ю працівників, особливо в стресових чи фізично важких умовах.

- **Моніторинг рівня стресу:** Існують біометричні технології, які аналізують зміни в потовиділенні, частоті серцебиття, а також інші показники, які вказують на стрес або емоційне перенавантаження. Це дозволяє своєчасно реагувати на зміни в стані працівника та надавати йому необхідну допомогу.

3. Моніторинг фізичного стану працівників

Для робіт, що вимагають великих фізичних навантажень або довготривалої фізичної активності, біометричні пристрої можуть допомогти контролювати фізичний стан працівника, виявляючи ознаки втоми або перенавантаження:

- **Моніторинг температури тіла:** Біометричні пристрої можуть відстежувати підвищення температури, що вказує на перегрів або інші фізіологічні проблеми, особливо в умовах високих температур або при виконанні важких фізичних робіт.

- **Вимірювання рівня кисню в крові:** Пульсоксиметри можуть допомогти виявити ранні ознаки кисневого голодування або інших проблем з диханням.

4. Профілактика нещасних випадків і зниження травматизму

Завдяки постійному моніторингу біометричних даних, компанії можуть швидше реагувати на потенційно небезпечні ситуації, знижуючи ризик травм або серйозних захворювань серед працівників:

- **Попередження про фізичне перенавантаження:** Системи, що контролюють рівень втоми та фізичний стан, можуть автоматично попереджати працівників або керівництво про необхідність перерви, знижуючи ризик травм через перевтому.

- **Зниження стресових ситуацій:** Своєчасне виявлення стресу може допомогти знизити рівень тривоги серед працівників, а також покращити їхнє самопочуття і продуктивність.

5. Аналіз даних і покращення умов праці

Дані, зібрані за допомогою біометричних технологій, можуть бути використані для аналізу та покращення умов праці на підприємствах:

- **Моніторинг робочих навантажень:** Зібрані біометричні дані можуть допомогти визначити, які працівники або робочі зміни піддаються найбільшим фізичним та психологічним навантаженням. Це дає змогу оптимізувати робочі процеси і графіки, знижуючи ризик перенавантажень.

- **Оцінка ефективності програм здоров'я:** Аналітика біометричних даних може допомогти оцінити, як різні програми для поліпшення здоров'я працівників (фізичні тренування, психологічна підтримка тощо) впливають на їхній загальний стан і продуктивність.

Доповнена реальність (AR) — це технологія, яка дозволяє накладати віртуальні елементи на реальний світ, створюючи інтерактивне середовище для користувача. В охороні праці AR-технології використовуються для підвищення рівня безпеки, покращення навчання працівників та зниження ймовірності нещасних випадків. Ось як саме доповнена реальність може бути застосована в цій галузі:

1. **Навчання працівників.** Доповнена реальність значно покращує процес навчання, надаючи можливість працівникам освоювати нові навички або отримувати інструкції в реальному часі в умовах реального робочого середовища:

- **Інтерактивні інструкції:** AR дозволяє накладати віртуальні інструкції або підказки на реальні об'єкти, які працівники використовують на робочому місці. Наприклад, на екрані окулярів AR можуть з'являтися підказки про те, як правильно використовувати обладнання або виконувати конкретні операції.

- **Тренування в реальних умовах:** AR дозволяє створити віртуальне середовище, яке імітує робочі умови, де працівники можуть тренуватися без ризику для безпеки. Це особливо корисно для навчання в складних чи небезпечних ситуаціях, де прямий досвід може бути небезпечним.

2. **Візуалізація ризиків.** Доповнена реальність дозволяє візуалізувати потенційні небезпеки, що існують в робочому середовищі. Це дає змогу працівникам вчасно ідентифікувати й уникати загроз:

- **Віртуальні попередження:** Під час виконання завдань у реальному часі, AR може відображати попередження або візуальні маркери, що вказують на потенційні небезпеки — наприклад, зони з підвищеним рівнем шуму, токсичних газів чи високої температури.

- **Моделювання аварійних ситуацій:** AR може симулювати різні надзвичайні ситуації, такі як пожежі, витоки газу чи аварії, і надавати працівникам покрокові інструкції щодо їх дій у разі виникнення цих ситуацій.

3. **Інструкції з техніки безпеки в реальному часі.** Вивчення техніки безпеки — це важливий аспект забезпечення безпеки працівників. AR-технології можуть надати працівникам необхідні інструкції по безпеці в реальному часі, коли це найнеобхідніше:

- **Персоналізовані інструкції:** Коли працівник виконує певне завдання, AR може надавати індивідуальні інструкції та рекомендації, що стосуються саме цього процесу. Наприклад, при використанні важкої техніки чи складних інструментів, на екрані AR можуть з'являтися інструкції з безпеки або навіть вказівки щодо конкретних дій.

- **Візуалізація процесу:** Інструкції з техніки безпеки можуть бути візуалізовані у вигляді 3D моделей чи анімацій, що полегшує їхнє сприйняття. Це особливо

корисно при навчанні роботи з новими чи складними системами, де традиційні інструкції не завжди дають чітке уявлення.

4. Тренування та підвищення кваліфікації. AR є потужним інструментом для проведення тренувань у безпечному і контрольованому середовищі, що дозволяє відпрацьовувати складні або небезпечні ситуації без реального ризику:

- **Тренування з аварійних ситуацій:** AR дає змогу створювати віртуальні аварійні ситуації (наприклад, пожежу або витік газу) в реальному робочому середовищі, щоб працівники могли вчитися реагувати на них без фізичної небезпеки. Це також допомагає підвищити рівень готовності до надзвичайних ситуацій.

- **Віртуальні симуляції:** Для працівників, які працюють з важким обладнанням або в умовах високих ризиків (наприклад, на висоті або в закритих просторах), AR-технології дозволяють проводити симуляції для підвищення кваліфікації. Наприклад, перед реальним завданням працівники можуть пройти через симуляцію робочого процесу або аварійної ситуації.

5. Підвищення продуктивності та безпеки через зворотній зв'язок. AR-технології дозволяють отримувати зворотний зв'язок у реальному часі, що допомагає працівникам коригувати свою поведінку або робочий процес:

- **Моніторинг продуктивності:** Окуляри чи інші пристрої AR можуть відстежувати, як ефективно працівник виконує завдання, та надавати рекомендації для поліпшення швидкості та точності роботи.

- **Аналіз помилок:** Якщо працівник робить помилку, AR може негайно відобразити це на екрані й запропонувати правильний спосіб виконання завдання.

6. Покращення командної роботи. В умовах, де необхідна командна взаємодія, AR може допомогти у координації дій:

- **Спільні тренування:** Кілька працівників можуть одночасно перебувати в AR-навчанні та бачити однакові віртуальні інструкції або попередження. Це особливо корисно для роботи в команді, де спільні дії важливі для забезпечення безпеки.

- **Віртуальні інструкції для віддалених працівників:** У випадку, коли працівники працюють у віддалених або небезпечних зонах, AR може бути використана для надання їм віртуальних інструкцій та підтримки у реальному часі через віддалене підключення.

- **Дистанційний моніторинг та управління** — це важливі аспекти сучасних цифрових технологій, які дозволяють ефективно контролювати стан безпеки на виробництві, попереджати аварії та автоматизувати різноманітні управлінські функції. Завдяки використанню сенсорних систем і технологій Інтернету речей (IoT), компанії можуть оперативно отримувати дані про умови на робочому місці та реагувати на потенційні небезпеки без необхідності фізичної присутності на місці. Ось як саме ці технології можуть бути застосовані в охороні праці:

1. Моніторинг безпеки на виробництві в реальному часі

Системи дистанційного моніторингу дозволяють збирати та аналізувати дані з численних сенсорів, що встановлені в робочих зонах, для забезпечення безпеки працівників. Це дозволяє вчасно виявляти відхилення від нормальних умов і попереджати про потенційні небезпеки:

- **Моніторинг умов навколишнього середовища:** Сенсори можуть вимірювати температуру, вологість, рівень пилу, концентрацію токсичних газів,

рівень шуму та інші фактори, що можуть впливати на безпеку працівників. У разі перевищення допустимих норм, система автоматично сповіщає про небезпеку та може активувати аварійні системи (наприклад, вентиляцію або пожежогасіння).

- **Розпізнавання аномалій:** На основі даних з сенсорів, спеціальні алгоритми можуть аналізувати показники та виявляти аномальні ситуації (наприклад, різке підвищення температури чи зміни в рівні кисню), що дозволяє своєчасно реагувати на потенційні загрози.

2. Попередження аварій

Дистанційний моніторинг допомагає своєчасно виявляти аварійні ситуації до того, як вони стануть критичними. Це особливо важливо для великих підприємств з потенційно небезпечними умовами праці (наприклад, хімічні заводи, гірничі підприємства, атомні станції).

- **Прогнозування аварій:** Системи можуть використовувати аналіз даних для прогнозування аварій або несправностей на основі змін у параметрах роботи обладнання чи умов навколишнього середовища. Наприклад, аналіз вібраційних датчиків може допомогти виявити наближення поломки або несправності на машинах, що дозволяє уникнути аварії.

- **Автоматизовані оповіщення:** Коли виникає загроза аварії (пожежа, витік газу, надмірний рівень шуму чи інші небезпечні фактори), система може негайно сповістити персонал і керівництво через різні канали зв'язку (сигналізації, електронна пошта, SMS-повідомлення).

3. Автоматизація звітності та управлінських функцій.

Системи дистанційного моніторингу значно спрощують процес управління та звітності на підприємстві:

- **Автоматичне збирання даних:** Сенсори, що працюють в реальному часі, автоматично зберігають дані, такі як показники температури, тиску, вологості, рівня газів тощо. Це дозволяє створювати детальні звіти без необхідності ручного збору інформації.

- **Аналіз і звітність:** Зібрані дані можуть бути автоматично оброблені за допомогою аналітичних інструментів для створення звітів про стан безпеки, ефективність роботи обладнання, витрати енергії тощо. Це значно спрощує процеси планування, прийняття рішень і покращує управлінську ефективність.

4. Оптимізація виробничих процесів і забезпечення безпеки.

Використання дистанційного моніторингу дозволяє не лише покращити безпеку, а й оптимізувати самі виробничі процеси:

- **Реальний моніторинг обладнання:** За допомогою сенсорів можна відстежувати стан машин і обладнання (наприклад, вібрації, температура, рівень палива тощо), що дозволяє своєчасно проводити технічне обслуговування і запобігти аваріям, пов'язаним з поломками.

- **Підвищення ефективності виробництва:** Дані, що надходять від сенсорів, дозволяють виявити неефективні або енергозатратні процеси, що дозволяє коригувати робочі процеси для досягнення кращої продуктивності та зменшення витрат.

5. Дистанційне управління та контроль

Завдяки дистанційному моніторингу, керівники можуть приймати управлінські рішення без необхідності фізично перебувати на підприємстві:

- **Контроль за операціями на відстані:** Керівники можуть використовувати централізовану платформу для моніторингу всіх процесів на підприємстві та приймати рішення, ґрунтуючись на реальних даних (наприклад, перенаправлення ресурсів, зміна виробничих параметрів).

- **Підключення до системи з будь-якої точки світу:** Завдяки хмарним технологіям та інтеграції з мобільними додатками, керівництво може отримувати дані і контролювати ситуацію на виробництві навіть на відстані.

6. Інтеграція з іншими системами безпеки

Системи дистанційного моніторингу можуть бути інтегровані з іншими системами безпеки (наприклад, відеоспостереження, охоронні сигналізації), що дозволяє створити єдину екосистему безпеки:

- **Інтеграція з системами відеоспостереження:** Система може автоматично виявляти аномалії в поведінці персоналу або виявляти несанкціонований доступ до небезпечних зон, що дає змогу своєчасно реагувати на порушення.

- **Автоматичне сповіщення охорони та служб безпеки:** У разі аварійної ситуації або виявлення небезпеки, система може автоматично сповістити охорону або працівників, відповідальних за безпеку, про загрозу.

Штучний інтелект (AI) і машинне навчання (ML) стають потужними інструментами для покращення безпеки праці та управління ризиками на підприємствах. Використання AI для аналізу великих обсягів даних дозволяє виявляти потенційні загрози, прогнозувати аварії та оптимізувати робочі процеси для забезпечення кращих умов праці. Ось кілька способів, якими штучний інтелект і машинне навчання можуть бути застосовані в охороні праці:

1. Аналіз великих даних для виявлення ризиків

AI і машинне навчання дозволяють ефективно обробляти величезні обсяги даних, зібраних з різних сенсорів, камер, моніторингових систем і звітів. Це допомагає виявляти патерни та аномалії, які можуть свідчити про підвищений ризик аварії чи небезпеки:

- **Ідентифікація ризиків на основі історичних даних:** Алгоритми машинного навчання можуть аналізувати дані про попередні інциденти на підприємстві, такі як поломки обладнання, аварії чи нещасні випадки, і виявляти схожі умови, що можуть призвести до подібних ситуацій. Це дає змогу попереджати про можливі загрози в майбутньому.

- **Прогнозування аварій та поломок:** AI може прогнозувати можливі аварії чи поломки на основі зібраних даних про стан обладнання, зміни в параметрах роботи (температура, вібрація, тиск, тощо). Наприклад, якщо алгоритм виявляє, що певний параметр наближається до критичного рівня, система може попередити про необхідність обслуговування чи заміни обладнання.

- **Аналіз умов навколишнього середовища:** AI здатний обробляти дані від сенсорів, що вимірюють температуру, рівень вологості, токсичні гази, шум та інші фактори, і прогнозувати можливі загрози для здоров'я працівників (наприклад, зростання концентрації шкідливих речовин у повітрі).

2. Аналіз поведінки працівників

AI та ML можуть використовуватись для аналізу поведінки працівників на робочому місці, зокрема для виявлення потенційно небезпечних дій:

- **Розпізнавання відхилень від норм:** AI може аналізувати відео з камер спостереження чи дані з датчиків, щоб виявляти відхилення від стандартних процедур безпеки. Наприклад, система може зафіксувати, якщо працівник не використовує захисне обладнання (шолом, рукавички) або знаходиться в небезпечній зоні без належного захисту.

- **Прогнозування фізичних ризиків:** Використовуючи біометричні дані, такі як серцевий ритм або рівень стресу, AI може виявляти фізичні перенавантаження працівника або стресові стани, що можуть призвести до нещасних випадків. Це дає змогу своєчасно втрутитись і допомогти працівнику до того, як станеться інцидент.

3. Інтелектуальні системи раннього попередження

Використання AI дозволяє створювати системи, які можуть попереджати працівників і керівництво про потенційні загрози на основі аналізу різних факторів:

- **Прогнозування ризиків:** AI може на основі аналізу великих масивів даних виявляти тренди, які вказують на підвищену ймовірність аварії чи нещасного випадку. Це дозволяє підприємству вчасно вжити заходів для попередження інцидентів.

- **Інтелектуальне планування технічного обслуговування:** Штучний інтелект може допомогти в оптимізації графіка технічного обслуговування та ремонту обладнання, аналізуючи дані про його стан і визначаючи, коли найбільше ймовірно виникнення поломок. Це дозволяє своєчасно запобігти аваріям, знижуючи ймовірність простоїв.

4. Покращення умов праці через рекомендації

AI також може надавати рекомендації щодо поліпшення умов праці, ґрунтуючись на аналізі робочих процесів, поведінки працівників та стану навколишнього середовища:

- **Рекомендації щодо змін у робочих процесах:** AI може пропонувати зміни в організації праці, щоб зменшити навантаження на працівників або полегшити виконання небезпечних завдань. Наприклад, система може рекомендувати автоматизацію певних процесів або зміну розкладу роботи для зменшення стресу або перевантаження.

- **Оптимізація робочого середовища:** На основі аналізу даних про рівень освітленості, температури, вентиляції та інших факторів, AI може пропонувати поліпшення умов робочого середовища для підвищення комфорту і зниження ризиків для здоров'я працівників.

- **Індивідуальні рекомендації для працівників:** AI може аналізувати індивідуальні показники здоров'я працівників і давати рекомендації щодо змін у їхній роботі, наприклад, частіші перерви, зміна навантаження, використання спеціального обладнання для зменшення фізичних навантажень.

5. Покращення процесів навчання та тренувань

AI може бути використаний для персоналізації навчання та тренувань з охорони праці:

- **Індивідуальні тренінги:** Штучний інтелект може створювати індивідуальні програми навчання для працівників на основі їхніх навичок, досвіду та специфіки роботи, що дозволяє покращити ефективність навчання та забезпечити більш глибоке засвоєння технік безпеки.

- **Симуляції аварійних ситуацій:** AI може використовуватися для створення реалістичних симуляцій аварійних ситуацій, що дозволяє працівникам навчатися реагувати на надзвичайні ситуації в контрольованому середовищі без ризику для їхнього здоров'я.

6. Автоматизація звітності та управління

AI також може автоматизувати процеси звітності та управлінських функцій, зокрема:

- **Автоматизовані звіти:** AI може автоматично генерувати звіти щодо стану безпеки, виявлених ризиків, поломок і ремонтів, що дозволяє зменшити адміністративні витрати і підвищити оперативність у прийнятті рішень.

- **Моніторинг ключових показників безпеки:** AI може відстежувати ключові показники безпеки в реальному часі та створювати попередження для керівництва у разі необхідності вжиття заходів для покращення умов праці.

Цифрові платформи для навчання та сертифікації стають важливими інструментами для покращення безпеки праці, оскільки вони дозволяють працівникам легко та зручно проходити тренінги, отримувати необхідні знання та сертифікації без необхідності присутності на традиційних заняттях. Ось кілька переваг та можливостей, які ці платформи пропонують в контексті охорони праці:

1. Доступність навчання в будь-який час і в будь-якому місці

Завдяки цифровим платформам, працівники можуть проходити курси та тренінги у зручний для них час і в будь-якому місці. Це особливо важливо для підприємств з великою кількістю працівників, які працюють в різних змінах або віддалених регіонах:

- **Гнучкий графік навчання:** Вебінари, онлайн-курси та тренінги дозволяють працівникам проходити навчання без необхідності змінювати свій графік роботи або витрачати час на поїздки в навчальні центри.

- **Доступ до навчальних матеріалів:** Всі матеріали, включаючи відео, презентації, тестові завдання, доступні на платформі, що дозволяє працівникам навчатися в зручному темпі, переглядати матеріали кілька разів для кращого засвоєння.

2. Індивідуалізація навчання

Цифрові платформи часто мають можливість персоналізувати навчання відповідно до конкретних потреб працівників або специфіки роботи підприємства:

- **Персоналізовані курси:** Курси можуть бути адаптовані залежно від професії працівника, рівня знань та досвіду, щоб навчання було максимально ефективним.

- **Тематичні тренінги:** Працівники можуть вибирати курси, що відповідають конкретним ризикам або умовам їх роботи, наприклад, тренінги з використання спеціального обладнання, роботи в небезпечних зонах, надання першої допомоги тощо.

3. Мультимедійний підхід до навчання

Цифрові платформи можуть інтегрувати різноманітні мультимедійні ресурси для підвищення ефективності навчання:

- **Відео та анімації:** Відеороки, інструкції та анімації допомагають краще розуміти складні концепції та практичні навички, такі як правильне використання захисного обладнання або проведення евакуаційних заходів.

- **Інтерактивні тренажери та симуляції:** Онлайн-платформи можуть використовувати симуляції аварійних ситуацій, що дозволяє працівникам практикувати свої дії в безпечному середовищі без ризику для здоров'я.

4. Оцінка знань та автоматична сертифікація

Після проходження курсу працівники можуть скласти тести та отримати сертифікати, що підтверджують їхню кваліфікацію:

- **Тести та перевірка знань:** Платформи можуть автоматично перевіряти знання через тести після кожного модуля або в кінці курсу, забезпечуючи точну оцінку рівня засвоєння матеріалу.

- **Автоматичне видавання сертифікатів:** Після успішного проходження курсу, система автоматично видає сертифікат, який може бути завантажений або надісланий електронною поштою. Це дає можливість працювати без необхідності чекати на вручення сертифікатів в класах.

5. Інтерактивні вебінари та онлайн-семінари

Вебінари та онлайн-семінари забезпечують можливість інтерактивного навчання, де працівники можуть безпосередньо спілкуватися з експертами і задавати питання:

- **Залучення експертів:** Прямі онлайн-сесії з фахівцями з охорони праці дозволяють розглядати актуальні питання, ділитися досвідом і отримувати відповіді на питання в реальному часі.

- **Обговорення реальних кейсів:** Вебінари можуть бути побудовані на основі реальних ситуацій з виробництва, що дозволяє розглянути практичні аспекти безпеки та уникнення небезпек на робочому місці.

6. Аналітика та відстеження прогресу

Однією з ключових особливостей цифрових платформ є можливість відстеження прогресу навчання працівників:

- **Аналітика прогресу:** Керівники можуть відслідковувати, як працівники проходять курси, які модулі вивчені, а де потрібна додаткова увага. Це дозволяє оцінити ефективність навчання та коригувати програми навчання за потребою.

- **Регулярне оновлення матеріалів:** Цифрові платформи можуть автоматично оновлювати матеріали, щоб працівники завжди мали актуальну інформацію, особливо щодо змін у законодавстві або нових технологій у сфері безпеки.

7. Зниження витрат на навчання

Онлайн-курси та вебінари допомагають підприємствам знизити витрати на навчання та сертифікацію працівників, оскільки немає необхідності в оренді класів, оплаті за навчання в навчальних центрах або витрат на поїздки:

- **Зниження витрат на логістику:** Працівники можуть навчатися, не виїжджаючи зі свого робочого місця, що значно знижує витрати на організацію навчального процесу.

- **Масовий доступ до курсу:** Один курс може бути доступний для великої кількості працівників одночасно, що знижує вартість навчання на одиницю працівника.

8. Підвищення залученості та мотивації працівників

Онлайн-курси можуть бути більш інтерактивними і залучати працівників до процесу навчання, що підвищує їхню мотивацію:

- **Гейміфікація процесу навчання:** Впровадження елементів гейміфікації (бали, нагороди, лідерборди) може зробити процес навчання більш захоплюючим і мотивувати працівників до кращих результатів.

- **Можливість самостійного навчання:** Працівники можуть вибирати курси, які найбільше відповідають їхнім потребам, що сприяє підвищенню їхнього інтересу та мотивації.

Віртуальна реальність (VR) є потужним інструментом для підвищення безпеки праці, оскільки вона дозволяє створювати реалістичні симуляції небезпечних ситуацій без ризику для здоров'я працівників. Завдяки VR-технологіям, працівники можуть тренуватися та освоювати навички реагування на надзвичайні ситуації в умовах, які не можна відтворити в реальному житті, або в ситуаціях, де існує високий ризик для життя. Ось як VR використовується для підвищення безпеки на робочих місцях:

1. Тренування в реалістичних симуляціях небезпечних ситуацій

VR дозволяє створювати симуляції аварій, катастроф, пожеж, вибухів або інших надзвичайних ситуацій, які можуть виникнути на робочому місці. Це дозволяє працівникам тренуватися в безпечному середовищі, де вони можуть відпрацьовувати свої дії без шкоди для їхнього здоров'я:

- **Імітація пожеж та евакуацій:** У VR-середовищі можна створювати реалістичні пожежі на виробництві або в офісах, де працівники тренуються, як правильно евакуюватися, використовувати вогнегасники та реагувати на дим чи задимлення.

- **Робота з небезпечними матеріалами:** Тренування в VR дозволяють працівникам відпрацьовувати навички роботи з небезпечними речовинами або обладнанням, наприклад, з хімічними речовинами чи вибухонебезпечними матеріалами, де реальні умови можуть бути занадто небезпечними для тренувань.

2. Безпечне навчання складних або рідкісних ситуацій

Віртуальна реальність дозволяє відтворити ситуації, які можуть бути складними або рідкісними у реальному житті, але які все одно необхідно відпрацьовувати для забезпечення безпеки:

- **Симуляції рідкісних аварій:** Наприклад, при аварії на виробництві, коли вибух або пожежа є малоймовірними, але смертельно небезпечними, VR дозволяє навчити працівників, як правильно діяти в таких екстремальних умовах.

- **Ситуації з підвищеним ризиком:** Навчання з використанням VR дозволяє тренуватися у ситуаціях, де навіть невеликі помилки можуть мати серйозні наслідки, наприклад, при роботі з високовольтним обладнанням чи в умовах підвищеного шуму.

3. Покращення навичок прийняття рішень під тиском

В умовах віртуальної реальності працівники можуть тренувати свої навички прийняття рішень в екстремальних ситуаціях:

- **Тренування швидких реакцій:** VR-системи можуть створювати стресові ситуації, де працівникам необхідно швидко реагувати, приймати рішення та здійснювати правильні дії для запобігання аварії чи зниження наслідків.

- **Робота під час стресу та паніки:** Тренування в умовах стресу допомагає працівникам залишатися спокійними та приймати правильні рішення навіть в умовах паніки, коли потрібно діяти швидко.

4. Тренування з використанням спеціального обладнання

Віртуальна реальність дозволяє створювати симуляції роботи з дорогим, складним або потенційно небезпечним обладнанням:

- **Моделювання роботи з важким обладнанням:** Працівники можуть навчатися керувати важким обладнанням (кранами, підйомниками, машинами тощо) без ризику пошкодження або аварії.

- **Моделювання ситуацій з поломкою обладнання:** VR дозволяє створювати ситуації, коли обладнання виходить з ладу, що дозволяє працівникам відпрацьовувати навички з ремонту чи обслуговування в реалістичних умовах.

5. Аналіз і покращення поведінки під час навчання

У VR-платформах можна проводити аналіз поведінки працівників під час тренувань:

- **Аналіз рішень і реакцій:** Завдяки використанню сенсорів і відеозапису, тренери можуть аналізувати, як працівники реагують на різні ситуації, виявляти слабкі місця в їхніх діях та надавати індивідуальні рекомендації для покращення.

- **Персоналізація навчання:** VR-системи можуть адаптувати навчання під індивідуальні потреби працівника, зважаючи на його реакції та поведінку в процесі тренувань.

6. Можливість тренувати великий колектив працівників одночасно

Віртуальна реальність дозволяє проводити тренування для великих груп працівників одночасно, навіть якщо вони знаходяться в різних місцях:

- **Групові тренінги та симуляції:** За допомогою VR можна проводити групові тренінги, де працівники спільно реагують на аварійні ситуації, що дозволяє відпрацьовувати командну роботу в умовах стресу.

- **Тренування дистанційних працівників:** VR дозволяє організовувати тренування для працівників, які працюють у віддалених регіонах або на різних об'єктах, зберігаючи високу якість навчання.

7. Безпечне навчання на всіх етапах виробництва. Віртуальна реальність дозволяє створювати тренування для працівників на різних етапах виробничого процесу:

- **Інструктажі з безпеки на всіх етапах:** Працівники можуть пройти тренування по техніці безпеки на різних етапах роботи — від початкового інструктажу до практичного застосування навичок у реальних умовах.

- **Навчання з моніторингу і контролю:** Для працівників, які відповідальні за моніторинг стану безпеки, VR дозволяє відпрацьовувати навички виявлення небезпек і своєчасного реагування на них.

8. Зниження витрат на навчання та безпеку

Віртуальні тренажери значно знижують витрати на фізичне навчання та підготовку:

- **Заміна реальних тренувань:** VR дозволяє замінити фізичне навчання, яке може вимагати спеціальних умов або дорогих навчальних майданчиків, на дешевші віртуальні тренування.

- **Зниження ризиків та витрат на медичне обслуговування:** Оскільки працівники тренуються без реального ризику для здоров'я, знижується ймовірність отримання травм під час навчання.

Серед ключових напрямів використання цифрових технологій в охороні праці можна виділити:

1.1 Системи моніторингу безпеки

Інтеграція датчиків і технологій IoT (Інтернет речей) дозволяє в режимі реального часу відстежувати:

- Температуру, вологість, рівень шуму та інші параметри робочого середовища.
- Концентрацію шкідливих речовин у повітрі для запобігання отруєнням чи алергічним реакціям.
- Стан обладнання, що знижує ризик аварій та збоїв.

1.2 Програмні платформи для аналізу ризиків

Спеціалізоване програмне забезпечення дає змогу моделювати та прогнозувати небезпеки:

- Виявлення слабких місць у виробничих процесах.
- Створення інтерактивних карт небезпеки.
- Планування заходів з підвищення безпеки на основі аналізу отриманих даних.

1.3 Використання дронів

Безпілотні літальні апарати активно використовуються для:

- Інспекції важкодоступних або небезпечних для людини об'єктів, таких як висотні споруди чи глибокі шахти.
- Моніторингу стану великих територій, наприклад, на будівельних майданчиках або виробничих комплексах.
- Фіксації потенційно небезпечних ситуацій за допомогою відеозапису чи фотознімків.

1.4 Інтерактивне навчання

Використання технологій віртуальної (VR) та доповненої реальності (AR) відкриває нові можливості для підготовки працівників:

- Відтворення реалістичних сценаріїв надзвичайних ситуацій для відпрацювання дій.
- Інтерактивні тренінги для закріплення знань правил безпеки.

Цифрові технології не лише допомагають зберегти життя і здоров'я працівників, але й стають основою для довгострокового розвитку підприємств, підвищуючи їх конкурентоспроможність у сучасному світі.

Системи моніторингу безпеки

Системи моніторингу безпеки – це сучасні технологічні рішення, що дозволяють забезпечувати постійний контроль за умовами праці та станом робочого середовища. Завдяки використанню датчиків і технологій IoT (Інтернет речей), такі системи забезпечують оперативне реагування на можливі загрози, підвищуючи рівень безпеки та зменшуючи ризики для здоров'я працівників. Використання систем моніторингу безпеки на основі датчиків і технологій IoT (Інтернет речей) є інноваційним підходом до забезпечення безпечних умов праці. Такі системи дають змогу постійно відстежувати критичні параметри робочого середовища в режимі реального часу, що дозволяє своєчасно виявляти та запобігати потенційним небезпекам.

Системи моніторингу безпеки дійсно є важливим елементом для підвищення безпеки на робочих місцях. Вони використовують різноманітні датчики, такі як температурні, вологі, газові або навіть сенсори для виявлення небезпечних рівнів шуму чи пари. Інтеграція цих технологій в систему IoT дозволяє здійснювати постійний моніторинг у реальному часі, автоматично фіксувати зміни в умовах праці та миттєво попереджати про потенційні небезпеки. Крім того, такі системи можуть бути інтегровані з іншими технологіями, як-от автоматичні системи пожежогасіння, освітлення, або охоронні сигнали. Це дозволяє не лише реагувати на небезпеку, а й попереджати її, що зменшує ймовірність виникнення аварій та травм. Завдяки розвитку IT і можливостям для обробки даних, ці системи також стають більш адаптивними та здатними до аналізу великих обсягів інформації для прогнозування та запобігання загрозам у майбутньому. Ось ще частина тексту, яка може доповнити тему систем моніторингу безпеки: Системи моніторингу безпеки на робочих місцях не лише знижують ризики для здоров'я та життя працівників, але й допомагають компаніям відповідати вимогам законодавства щодо охорони праці. Сучасні технології дозволяють здійснювати автоматичне збирання даних і формування звітності, що значно спрощує процес контролю за умовами праці та своєчасним виявленням порушень. Завдяки інтеграції з хмарними технологіями, дані, отримані від датчиків, можуть зберігатися в реальному часі, що дає можливість оперативного доступу до інформації будь-де і будь-коли. У разі виникнення небезпечних ситуацій, системи можуть автоматично сповіщати відповідальних осіб через мобільні додатки або панелі управління, а також запускати необхідні дії для мінімізації загрози, наприклад, активувати системи вентиляції чи охолодження. Крім того, використання таких технологій дозволяє проводити аналітику і тренди щодо умов праці, що дає змогу не лише своєчасно реагувати на поточні проблеми, а й передбачати можливі труднощі у майбутньому. Наприклад, за допомогою алгоритмів машинного навчання можна виявляти аномалії або тенденції, які можуть свідчити про потенційні небезпеки, що дозволяє вжити превентивних заходів. Таким чином, системи моніторингу безпеки є важливим кроком у створенні безпечного робочого середовища, де кожен працівник може бути впевнений у своєму захисті, а компанія зменшує фінансові та репутаційні ризики.

Основні функції систем моніторингу:

1. Вимірювання ключових параметрів:

- Температура та вологість повітря для забезпечення комфортних умов роботи.
- Рівень шуму для захисту слуху працівників від шкідливого впливу.
- Концентрація шкідливих газів чи частинок у повітрі для попередження отруєнь і респіраторних захворювань.

2. Аналіз та передача даних:

- Інтеграція з хмарними платформами для обробки та збереження інформації.
- Автоматичне формування звітів і графіків на основі отриманих даних.
- Надсилання попереджувальних сигналів або сповіщень у разі перевищення встановлених меж.

3. Оперативне реагування:

- Система може запускати автоматичні протоколи безпеки, наприклад, вентиляцію у разі високої концентрації газів.
- Негайне сповіщення відповідальних осіб або працівників про небезпечні умови.

Переваги впровадження таких систем:

Зменшення впливу людського фактора у процесі контролю за умовами праці.

- Підвищення точності та швидкості виявлення ризиків.
- Поліпшення умов праці та підвищення рівня здоров'я працівників.
- Оптимізація витрат на забезпечення безпеки.

Системи моніторингу безпеки є важливим кроком до створення «розумного виробництва», де забезпечення безпеки праці стає не просто вимогою, а частиною корпоративної культури.

References:

- Ткачук К. Н. Основи охорони праці: підручник. 21-ше видання, доповнене та перероблене / М. О. Халімовський, В. В. Зацарний, Д. В. Зеркалов, Р. В. Сабарно, О. І. Полукаров, В. С. Коз'яков, Л. О. Мітюк. За ред. К. Н. Ткачука і М. О. Халімовського. К.: Основа, 2006. 448с.
<https://surl.li/ethazz>
- Шудренко І. В. Основи охорони праці: навч. посіб. Житомир: Видавець О. О. Євенок, 2016. 214 с.
URL: <https://surl.li/etnkbl>
- Інновації в сфері охорони і гігієни праці. URL: <https://surl.li/iphgtj>
- Корольчук М. С., Крайнюк, В. М. Теорія і практика професійного психологічного відбору: навч. посіб. для студентів вищих навч. закл. 2006. 536 с. URL: <https://surl.li/dopkro>
- «Про охорону праці»: Закон України No 2695-XII від 14.10.1992 (Редакція станом на 05.04.2015)
URL:<http://zakon5.rada.gov.ua/laws/show/2694-12>
- Білоус І.І. Поняття соціальної безпеки та її роль в системі національної безпеки держави. Ефективна економіка. 2019. No 3. URL: <https://surl.li/chtfc0> DOI: 10.32702/2307-2105-2019.3.41.2
- Мотайло О.В. Система національної безпеки держави. URL: <https://surl.li/cc/lkyuhj>
- Роль хмарних обчислень у зберіганні даних електронного навчання. URL: <https://surl.li/svyvve>
- Східне міжрегіональне управління Державної служби України з питань праці. URL: <https://surl.li/hafjoo>
- Центральне міжрегіональне управління Державної служби з питань праці. URL: <https://surl.li/nzctxi>
- Про охорону праці: Закон України від 14.10.1992 р. No 2694-XII (із змінами).
URL:<https://zakon.rada.gov.ua/laws/show/2694-12#Text>
- Агій Я. Ю. Охорона праці у галузі : навч. посіб. /Я. Ю. Агій, І. М. Лях. ; рец. : В. Ц. Жидецький, К. М. Кишко ; М-во освіти і науки України, ДВНЗ «Ужгородський національний університет». Вид. 2-ге допов., переробл. Ужгород : ДВНЗ «УжНУ», 2024. 211 с. URL: <https://surl.li/ujmccx>
- Батлук В. А., Кулик В. М., Яцюк Р. А. Охорона праці: навч. посібник. Львів: Видавництво Львівської політехніки, 2011. 388 с. DOI: <https://surl.li/riehfq>
- Запорожець О. І., Протоєрейський О. С., Франчук Г. М., Боровик І. М. Основи охорони праці. Підручник. К.: Центр учбової літератури, 2009. 264 с. DOI: <https://surl.li/vjsqvv>
- Охорона праці: навч. посіб. / З. М. Яремко, С. В. Тимошук, О. І. Третяк, Р. М. Ковтун; за ред. проф. М. Яремка. Львів: Видавничий центр ЛНУ імені Івана Франка, 2010. 374с. DOI: <https://surl.li/dwxhit>
- Катренко Л. А., Кіт Ю. В., Пістун І. П. Охорона праці. Курс лекцій. Практикум: Навч. посіб. Суми: Університетська книга, 2009. 540 с. URL: <https://kbg.pnu.edu.ua/wp-content/uploads/sites/96.pdf>
- Зеркалов Д. В. Безпека життєдіяльності. Навч. посіб. К.: Основа, 2011. 526с. URL: <https://surl.li/bokchh>
- Cempel, C., & Tomaszewski, F. (2001). Wytyczne dla systemów zarządzania bezpieczeństwem i higieną pracy ILO-OSH, wyd. IOP, Warszawa. URL: <https://surl.li/emzfxX>

- Ejdys, J., Lulewicz, A., & Obolewicz, J. (2000). Zarządzanie bezpieczeństwem w przedsiębiorstwie, pod red. Politechnika Białostocka, Białystok. DOI: <https://surl.li/sixinc>
- Korodecka, D. i in. (2000). Diagnostyka i projektowanie układów antropogenicznych, [w:] Nauka o pracy – bezpieczeństwo, higiena, ergonomia, Wyd. CIOP, Warszawa. DOI: <https://surl.li/yqsvpa>
- Kowalski, J., & Krzyśków, B. (2000). Procesy pracy – pojęcia podstawowe, geneza idei ochrony pracy [w:] D. Koradecka; Nauka o pracy – bezpieczeństwo, higiena, ergonomia, wyd. CIOP, Warszawa. DOI: <https://surl.li/lciffu>
- Makarewicz, R. (1996). Hałas w środowisku, Ośrodek Wyd. Naukowych PAN, Poznań. DOI: 10.5604/01.3001.0013.6382
- Sakun, M. M. (2012). Okhorona pratsi u tvarynnytsvi. Navchalnyi posibnyk dlia pidhotovky fakhivtsiv OKR “Spetsialist”, “Mahistr” zi spetsialnosti 7.130. 201, 8.130. 201 – zoonzheneriia. Odesa “Tsentr Media”. URL: <https://surl.li/ytrnbr> (in Ukrainian).
- Savchenko, L. H., Tsyvenkova, N. M., & Savchenko, V. M. (2016). Doslidzhennia rivnia vyrobnychoho ravmatyzmu i profzakhvoriuvanosti v haluzi tvarynnytsva ta pererobky produktii tvarynnytsva APK Ukrainy. Podilskyi visnyk: silske hospodarstvo, tekhnika, ekonomika, 25, 115–122. URL: <https://surl.li/sjqsii> (in Ukrainian).
- Tytyk, E. (2001). Projektowanie ergonomiczne, Wydawnictwo Naukowe PWN, Warszawa–Poznań.
- Wawszczak, W. (2007). Modele człowieka – Humanizacja techników, ale także Technicyzacja humanistów”, Referat na konferencji Forum Pracowników Nauki „Nauka-Etyka-Wiara”, Politechnika Łódzka, Rogowo. DOI: <https://doi.org/10.32718/nvlvet-a10041>
- Wyka, T. (2000). Diagnostyka układów antropometrycznych; w: Nauka o pracy – bezpieczeństwo, higiena, ergonomia, Red. D. Koradecka; wyd. CIOP; Warszawa. DOI: 10.37105/sd.26
- Yaroshovych, I. H., Chaikovskiy, B. P., Yaroshovych, T. S., & Shalko, A. V. (2020). Metodichni rekomendatsii z normatyvnoi dystsypliny “Okhorona pratsi u tvarynnytsvi” na temu: “Vymohy bezpeky do vyrobnychoho obladnannia, ekspluatatsii silskohospodarskoi tekhniki ta utrymannia tvaryn u silskohospodarskomu vyrobnytsvi”. Lviv. URL: <https://surl.li/gddwhd> (in Ukrainian).
- Zakon Ukrainy (1992). “Pro okhoronu pratsi”. Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1992, № 49, st. URL: <https://surl.li/zxfxiw>

CHAPTER 6. COMPETENCE-BASED APPROACH IN EDUCATIONAL MANAGEMENT: THEORY AND PRACTICE

Volodymyr BORYSOV

Candidate of Philology, Associate Professor,
Vice-Rector for Educational & Scientific Work,
H. S. Skovoroda Kharkiv National Pedagogical University (Kharkiv, Ukraine)

prorector_borysov@hnpu.edu.ua
<https://orcid.org/0000-0001-7468-727X>

Olena GRECHANYK

Candidate of Pedagogical Sciences, Associate Professor,
Head of the Department of Management and Economics,
H. S. Skovoroda Kharkiv National Pedagogical University (Kharkiv, Ukraine)

grechaniklena@ukr.net
<https://orcid.org/0000-0002-4671-0724>

Abstract. The monograph substantiates the relevance of the competence approach in educational management. The theoretical foundations of the use of the competence approach in the management of general secondary education institutions are revealed: the essence of the competence approach and the peculiarities of its implementation in an educational institution are clarified; the advantages and disadvantages of this approach are identified, the need to take them into account when implementing in practice is proved. The state of management of an educational institution on the basis of the competence approach is analysed, for which the diagnostic tools are streamlined and partially developed, a research programme is drawn up, and an expert group is formed. Thus, the level of managerial competence of the head of a basic educational institution, the level of management of an educational institution, the level of development of the creative potential of the teaching staff, the level of management of the development of teachers' creative competence were determined. Based on the results of the analysis, a targeted project to improve the management of an educational institution based on a competency-based approach has been developed. The stages of project implementation and the implementation period of one year are outlined. An implementation plan for project activities has been developed. An expert evaluation of the project was carried out according to such criteria as relevance, systematicity, realism, completeness, psychological support, innovation, productivity, optimality, reflexivity, and personal effectiveness. The expert group recommended the project for implementation in the practice of the educational institution.

Keywords: management, competences, educational institution, qualimetric model, target project, creative competence, creative potential, quality of education, quality of educational activity.

КОМПЕТЕНТІСНИЙ ПІДХІД В ОСВІТНЬОМУ МЕНЕДЖМЕНТІ: ТЕОРІЯ І ПРАКТИКА

Анотація. У монографії обґрунтовано актуальність компетентісного підходу в освітньому менеджменті. Розкрито теоретичні засади використання компетентісного підходу в управлінні закладом загальної середньої освіти: уточнено суть компетентісного підходу й особливості його реалізації в закладі освіти; визначено переваги й недоліки цього підходу, доведено необхідність їх урахування під час впровадження в практичну діяльність. Проаналізовано стан управління закладом освіти на засадах компетентісного підходу, для чого впорядковано й частково розроблено діагностичний інструментарій, складено програму дослідження, сформовано експертну групу. Так, встановлено рівень управлінської компетентності керівника базового закладу освіти, рівень управління закладом освіти, рівень розвитку творчого потенціалу педагогічного колективу, рівень управління розвитком творчої компетентності педагогів. За результатами проведеного аналізу розроблено цільовий проєкт з удосконалення управління закладом освіти на засадах компетентісного підходу. Окреслено етапи впровадження проєкту та термін реалізації – один рік. Розроблено план реалізації заходів проєкту. Здійснено експертне оцінювання проєкту за такими критеріями, як актуальність, системність, реалістичність, повнота, психологічний супровід, інноваційність, продуктивність, оптимальність, рефлексивність та особистісна результативність. Експертною групою проєкт було рекомендовано до реалізації в практику роботи закладу освіти.

Ключові слова: управління, компетенції, заклад освіти, кваліметрична модель, цільовий проєкт, творча компетентність, творчий потенціал, якість освіти, якість освітньої діяльності.

Вступ. Компетентісний підхід в освітньому менеджменті з кінця XX століття залишається надзвичайно актуальним, оскільки сучасна освіта потребує не лише передання знань, а й формування ключових компетентностей у керівників і педагогів. Це сприяє підвищенню ефективності управління закладами освіти й забезпечує їхній розвиток у динамічних умовах.

Упровадження компетентісного підходу відповідає міжнародним тенденціям і європейським стандартам освіти, зокрема вимогам Європейської рамки кваліфікацій. Це сприяє гармонізації освітнього менеджменту та підвищенню якості освітнього процесу. Компетентісний підхід також забезпечує ефективне прийняття управлінських рішень, стратегічне планування та розвиток освітніх закладів відповідно до сучасних викликів.

Керівники закладів освіти потребують нових підходів до управління, орієнтованих на лідерство, критичне мислення, креативність та ефективну комунікацію. Це особливо важливо в умовах цифровізації, коли освітні процеси зазнають суттєвих змін, а управлінці мають адаптуватися до нових технологічних і педагогічних викликів.

Окрім того, актуальність теми зумовлена необхідністю успішного впровадження реформ у сфері освіти. Керівникам закладів освіти важливо розвивати управлінські компетентності, щоб ефективно реалізовувати нові освітні стандарти та програми. Отже, дослідження компетентісного підходу в освітньому менеджменті є важливим кроком до підвищення якості освіти, освітньої діяльності й формування ефективної системи управління.

Об'єкт дослідження: особливості реалізації компетентнісного підходу в освіті.

Предмет дослідження: управління закладом освіти на засадах компетентнісного підходу.

Аналіз наукової літератури засвідчив, що питанням розвитку професійної компетентності педагогів присвячені наукові дослідження вітчизняних та зарубіжних науковців: Н. Бібік, О. Гречаник, В. Григораша, Г. Єльнікової, Т. Куценко, Л. Лузан, О. Онаць, О. Темченко, Т. Хлебнікової та інших. Теоретичні та практичні аспекти управління освітніми системами взагалі й закладами загальної середньої освіти зокрема представлено в роботах таких науковців, як Г. Єльнікова, Г. Кравченко, В. Лунячек, О. Мармаза, Т. Махиня, В. Маслов, В. Олійник, В. Пікельна, Г. Полякова, О. Почуєва, З. Рябова, Є. Хриков, Р. Черновол-Ткаченко та інших. Модернізація змісту освіти розкрита в працях Л. Гриневич, В. Кременя, О. Ляшенко, Н. Ничкало, Р. Шияна та інших. Проблему управлінської компетентності керівника закладу освіти досліджували М. Бегей, В. Бондар, Л. Даниленко, Л. Зеленська, С. Кіриченко, В. Маслов, М. Шленьова та інші. Проте необхідно уточнити суть управлінської компетентності керівника з огляду на зміни вимог до нього та стандартизацію діяльності, а також запропонувати механізми її вдосконалення та підвищення рівня управління закладом освіти.

Мета дослідження: за результатами аналізу розробити цільовий проєкт з удосконалення управління закладом освіти на засадах компетентнісного підходу.

Відповідно до поставленої мети було визначено такі *завдання дослідження*:

- 1) уточнити суть компетентнісного підходу й особливості його реалізації в закладі освіти;
- 2) проаналізувати стан управління закладом освіти на засадах компетентнісного підходу;
- 3) розробити цільовий проєкт з удосконалення управління закладом освіти на засадах компетентнісного підходу та здійснити його експертизу.

Досягнення поставленої мети й виконання сформульованих завдань було здійснено за допомогою комплексу *методів*, як-от: *теоретичних* (вивчення нормативно-правових, концептуальних, інструктивних, методичних документів, на основі яких здійснюють управління закладом освіти та його структурними одиницями; абстрагування, що сприяло визначенню й узагальненню підходів і спроб до розв'язання досліджуваної проблеми); *емпіричних* (спостереження, анкетування, бесіди, опитування, тестування; метод педагогічного моделювання); *методів математичної статистики й оброблення результатів*.

Джерельну базу дослідження складають:

- нормативні документи, що визначають і регулюють процеси у сфері менеджменту освітніх організацій: Закон України «Про освіту», Закон України «Про повню загальну середню освіту»; Концепція «Нова українська школа»;
- наукова періодика, у тому числі: «Актуальні питання у сучасній науці», «Вісник науки та освіти», «Наукові інновації та передові технології»;
- матеріали науково-практичних конференцій: «Розвиток системи управління організацією: Європейська практика та досвід України» (Харків, 2024), «Управління організацією в сучасних реаліях міжнародного співробітництва» (Харків, 2024), «Використання технологій менеджменту якості в управлінні закладами освіти»

(Тернопіль, 2024) та ін.;

- фонди бібліотек (Національна бібліотека України імені В. І. Вернадського, Харківська державна наукова бібліотека України імені В. Г. Короленка тощо);
- матеріали мережі Інтернет з окресленої проблеми.

Наукова новизна одержаних результатів дослідження полягає в тому, що *вперше*: синтезовано діагностичні методики оцінювання управління закладом освіти на засадах компетентнісного підходу; запропоновано цільовий проєкт з удосконалення управлінської діяльності відповідно до предмету дослідження.

Подальшого *розвитку* набули ідеї компетентнісного, діяльнісного, особистісного й системного підходів.

Практичне значення отриманих результатів дослідження полягає в упорядкуванні цільового проєкту з удосконалення управління закладом освіти на засадах компетентнісного підходу й можливостей його реалізації в закладах освіти з урахуванням специфіки актуальних проблем.

Основні результати дослідження було впроваджено в управлінську діяльність КЗ «Харківська гімназія № 92 Харківської міської ради». Результати дослідження можуть стати в пригоді керівникам закладів освіти різних типів, у системі підвищення кваліфікації керівних кадрів освіти, у процесі підготовки здобувачів освіти другого (магістерського) рівня вищої освіти зі спеціальностей А1 Освітні науки, А4 Середня освіта, А5 Професійна освіта, D3 Менеджмент.

1. Теоретичні засади компетентнісного підходу в управлінні закладом освіти

1.1 Поняття та сутнісні характеристики компетентнісного підходу в управлінні закладом освіти

Сучасна освіта є не просто інструментом передавання знань, а засобом формування особистості, яка здатна до самостійного розвитку, адаптації до змін й успішної інтеграції в суспільство. Зараз потрібно виховувати людей, які не лише мають знання та навички, але й володіють такими важливими якостями, як критичне мислення, креативність, здатність до комунікації, толерантність і соціальна відповідальність. Такий підхід сприятиме їхньому гармонійному розвитку, успішній кар'єрі й активній участі в розвитку суспільства.

Компетентнісний підхід у педагогічній освіті – це відповідь на виклики сучасного суспільства, що потребує фахівців, готових до самостійної роботи і постійного розвитку. Він передбачає організацію навчання, виховання й розвитку, що спрямована на формування в майбутніх педагогів комплексу компетенцій, необхідних для ефективної діяльності. Завдяки поєднанню теорії і практики управління отримують досвід вирішення реальних педагогічних задач, що дозволяє їм бути готовими до роботи в сучасному закладі загальної середньої освіти (далі – ЗЗСО) (Г. Єльнікова, 2010).

Поняття «компетентнісний підхід», «компетенція» мають свої витоки в галузі менеджменту, і згодом були успішно адаптовані до сфери освіти. Цей підхід став «одночасно і реакцією, і джерелом компетентнісного підходу» (О. Попова, 2012).

Отже, компетентнісний підхід в освіті дослідники визначають як сукупність загальних принципів, що регулюють постановку освітніх цілей, відбір змісту навчання, організацію освітнього процесу й оцінювання результатів. Під час

проектування освітнього процесу на основі компетентнісного підходу ключовим елементом побудови змісту є професійне завдання (В. Луговий, 2009).

Компетентнісний підхід робить акцент на практичному застосуванні знань. Його мета – сформувати в людини здатність самостійно розв’язувати різноманітні проблеми, адаптуючись до змінних умов. Замість того щоб просто передавати інформацію, цей підхід спрямований на розвиток умінь аналізувати ситуацію, приймати рішення й діяти. Відтак компетентнісний підхід формує не просто освічених людей, а особистостей, здатних до постійного розвитку та самовдосконалення (А. Синиченко, 2016).

Популярність компетентнісного підходу сприяла виникненню різноманітних теоретичних досліджень (Ю. Поскрипко, О. Данченко, 2019; *Розвиток системи...*, 2021), незважаючи на які, дуже складно в сучасній літературі знайти чітко визначені трактування сутності понять «компетенція» та «компетентність», їх принципових відмінностей, однозначно сформовані класифікації. Це актуалізує подальше дослідження цього питання, спрямованого на розкриття сутності базових понять компетентнісного підходу, виявлення їх видів із урахуванням особливостей діяльності працівників, аналіз методик відбору та залучення персоналу до виконання завдань стратегічної спрямованості, розроблення напрямів їх удосконалення.

Усвідомлення розмаїття визначень понять «компетенція» та «компетентність», підходів щодо їх використання в управлінні можливе лише за умови розуміння джерела й умов їх виникнення. Ці поняття активно використовують як в освіті, так і в менеджменті. Хоча ці сфери тісно пов’язані, їхнє розуміння компетентнісного підходу має певні відмінності. Наше дослідження ми маємо намір зосередити на особливостях застосування компетентнісного підходу саме в контексті управління.

Компетентнісний підхід, що зародився у 70-х роках ХХ століття в США, став своєрідною відповіддю на виклики часу. У розвитку компетентнісного підходу виокремлюють три етапи, що відображено в табл. 1.1.

Таблиця 1.1

Періодизація становлення та розвитку компетентнісного підходу (О. Мармаза, 2015)

Період	Основні досягнення
I етап (1960–1970 роки)	Становлення й уточнення понять «компетенція» і «компетентність» як інструментів оцінювання потенціалу працівників
II етап (1970–1996 роки)	Використання категорій «компетенція» і «компетентність» в управлінні, вивчення їхнього впливу на професійну діяльність людини та конкурентоспроможність організації
III етап (1996 рік – по цей час)	Компетентнісний підхід до особистості набув офіційного статусу, знайшовши своє відображення в міжнародних освітніх документах. Розвиток компетентнісного підходу в управлінні

Ідея про те, що справжню цінність становлять не лише знання, а й уміння їх застосовувати, уперше була висловлена Ноамом Хомським. Він увів термін «компетенція» для позначення здатності людини використовувати свої знання на

практиці. Цей підхід, що спирався на ідеї гуманітарних наук, заклав основу для подальших досліджень і став фундаментом для розуміння компетентності як багатогранної характеристики людини, що включає не лише знання, а й навички, уміння й особистісні якості, необхідні для успішної діяльності в різних сферах життя (N. Chomsky, 1965).

Під час другого етапу в 70-90-х роках ХХ століття сфера застосування понять «компетенція» та «компетентність» значно розширилася. Якщо спочатку їх асоціювали з мовними навичками, то згодом почали використовувати для опису широкого спектру знань, умінь і особистісних якостей, необхідних для успішної професійної та соціальної діяльності, в управлінні. Дослідники намагалися зрозуміти, як формувати, розвивати та використовувати компетенції для досягнення успіху як на індивідуальному, так і на організаційному рівні. Особливу увагу приділяли впливу компетенцій на ефективність роботи, кар'єрне зростання й загальний успіх організацій.

Девід Макклелланд, один із тих, хто започаткував управління персоналом, запропонував інноваційний підхід, який дозволяє оцінювати працівників на основі їхніх компетенцій. Цей підхід, запропонований у 1973 році, передбачає аналіз реальної поведінки людини на робочому місці та дозволяє визначити, які саме навички та знання сприяють її успіху. Компетентнісний підхід є більше гнучким та індивідуальним порівняно з традиційними методами оцінювання, оскільки він не обмежується перевіркою загальних знань або досвіду, а фокусується на конкретних результатах роботи. Цей підхід має широке застосування в сучасному управлінні персоналом і дозволяє ефективніше відбирати кандидатів, розвивати персонал і планувати кар'єру працівників (D. McClelland, 1973).

Брати Спенсери розглядали компетенції як фундаментальні якості людини, які визначають її ефективність у виконанні роботи. Вони запропонували системний підхід до розуміння компетенцій, підкресливши, що не всі характеристики людини можуть бути віднесені до компетенцій (L. Spenser, S. Spenser, 1993). Спенсери розробили методику, яка дозволяє ідентифікувати ключові компетенції для різних професійних ролей, і створили світову базу даних, що містить опис цих компетенцій, і словник професійних компетентностей (із поведінковими індикаторами). Їхні дослідження зробили значний внесок у розвиток теорії та практики управління персоналом.

Вагомий вклад у розвиток компетентнісного підходу належить Р. Бояцису, який поняття «компетенція» і «компетентність» пов'язав із поняттям «ефективна робота». Він вивчав характеристики, що дозволяють менеджерам ставати успішними, визначив 19 ключових компетенцій, що сприяють ефективній роботі. Відповідно до результатів його досліджень, наявність цих компетенцій є необхідною, але недостатньою умовою успіху. Важливо, щоб вони відповідали вимогам конкретної посади й організаційної культури суб'єкта господарювання. Робота Бояциса стала важливим внеском у розвиток теорії менеджменту та широко використовується для оцінювання й розвитку менеджерського потенціалу (Новий освітній простір, 2019).

Джон Равен розширив розуміння компетентнісного підходу, підкресливши, що це не просто сума знань і навичок, а комплексний феномен, який включає в себе також систему особистих цінностей. За його визначенням, компетентність – це здатність

людини ефективно діяти у своїй професійній сфері, досягаючи високих результатів завдяки своїм знанням, навичкам та внутрішній мотивації (*Л. Гуцан, 2013*). Дж. Равен, один із провідних дослідників у цій галузі, запропонував детальну класифікацію компетенцій (усього 37), що включала такі аспекти, як здатність до прийняття рішень, самостійне мислення, емоційний інтелект та інші.

Інший американський учений Ч. Вудраф запропонував своє бачення поняття «компетенція» і «компетентність»: компетенція – це сукупність конкретних дій та поведінки, необхідних для виконання роботи з урахуванням компетентностей. Компетентність же він визначив як рівень якості виконання цих дій. За його концепцією, компетенції задають рамки, у яких людина діє, а компетентність демонструє, наскільки ефективно людина використовує ці рамки. Отже, Вудраф підкреслив важливість не тільки знань і навичок, але й здатності застосовувати їх на практиці для досягнення поставлених цілей.

Поняття «ключові компетенції організації» було вперше введено К. Прахаладом та Г. Хемелом, засновниками компетентнісного підходу в управлінні. Вони визначили їх як «колективне знання організації, особливо щодо того, як скоординувати різні виробничі навички, уміння й різні технологічні потоки» (*К. Рудніцька, 2016*).

Ця концепція була розвинена іншими дослідниками, такими як М. Портер та М. Армстронг, які підкреслили, що ключові компетенції є результатом еволюції організації та дозволяють їй досягати конкурентних переваг. Розуміння своїх ключових компетенцій є важливим для будь-якої організації, оскільки дозволяє їй ефективно використовувати свої ресурси та досягати стратегічних цілей.

Процеси глобалізації та інтеграції європейської освіти стали потужним стимулом для розвитку компетентнісного підходу, особливо у сфері професійної освіти. Українські вчені І. Бех, Н. Бібік, Л. Ващенко, О. Локшина, І. Єрмаков, О. Овчарук, Л. Парашенко, О. Пометун, О. Савченко, С. Трубацова та інші активно долучилися до цих досліджень, спрямувавши свої зусилля на модернізацію національної системи освіти та підвищення її якості (*Н. Бібік, 2015; О. Варецька, 2015; Л. Гуцан, 2013; Г. Єльнікова, 2010*).

Згідно з дослідженнями Н. Бібік, розвиток компетентнісного підходу вимагає комплексного переосмислення освітнього процесу. Це передбачає оновлення навчальних програм, упровадження нових методів оцінювання та індивідуалізацію навчання. Мета таких змін – створити умови для розвитку кожного учня та підготовки його до життя в сучасному світі (*Н. Бібік, 2015*).

Третій етап розвитку компетентнісного підходу (90-ті роки ХХ століття – сьогодні) був тісно пов'язаний із потребами підготовки фахівців, які відповідають вимогам сучасного ринку праці та можуть успішно конкурувати на міжнародній арені.

Із 1996-го року міжнародні організації, такі як ЮНЕСКО та Рада Європи, офіційно визнали необхідність формування ключових компетенцій (key competencies) у школярів як основи для успішної професійної діяльності та подальшого навчання. Цю тенденцію підтверджують дослідження Організації економічного співробітництва та розвитку (OECD), розпочаті в 1997-ому році в рамках проєкту

«Визначення та відбір компетентностей: концептуальні засади» DeSeCo, які були спрямовані на визначення ролі компетентностей в європейській освіті.

Болонська декларація, що запровадила компетентнісний підхід в освіту, стала важливим кроком у розвитку системи підготовки фахівців. Перехід від предметної диференціації до міждисциплінарної інтеграції дозволяє формувати в студентів комплекс компетенцій, необхідних для успішної роботи в сучасному світі. Розвиток лідерських якостей, креативності та здатності до міждисциплінарного мислення є ключовими факторами підвищення ефективності управління та сприяє досягненню стратегічних цілей організацій.

Компетентнісний підхід, згідно з Болонським процесом, охоплює такі аспекти:

- а) компетенції є інструментом для чіткого опису академічних та професійних профілів;
- б) мова компетенцій фокусується на реальних результатах освітнього процесу;
- в) зосередження стандартів і навчальних планів на результатах освіти забезпечує порівнянність та прозорість кваліфікацій в європейському просторі.

Різноманітність підходів до управління відображає багатовікову еволюцію менеджменту. Кожен із них має свої переваги та недоліки, які проявлялися в різні історичні періоди. Однак, синтезуючи найкращі практики різних шкіл управління, сучасні менеджери можуть створити гнучку й ефективну систему управління, яка дозволить досягти стратегічних цілей організації (*О. Савченко, 2010; О. Язловецька, 2022*).

Ще одне питання, яке турбує дослідників, полягає в чіткому розмежуванні понять «компетенція» та «компетентність». Теоретичний аналіз підтвердив висновок про їх взаємопов'язаність і взаємообумовленість, однак, не повну їх тотожність. Компетенції, найчастіше, науковці розглядають як: сукупність наявних знань, умінь, навичок особистості; комплекс необхідних індивідуальних характеристик та професійно важливих якостей особистості; модель поведінки людини, що, у будь-якому разі, впливають на рівень виконання певної діяльності. З огляду на це, доцільно компетенції розглядати як сукупність знань, умінь, навичок, загальної і професійної ерудиції та інтуїції, поведінкових компонентів, що формують досвідченість особистості в певному колі питань і створюють потенційну можливість їх ефективного вирішення, що підвищує вірогідність отримання запланованих результатів діяльності. Тобто можна сказати, що наявність у працівника певних компетенцій створює його внутрішній потенціал та визначає так звану ступінь його готовності до ефективної роботи в конкретній робочій ситуації. Щодо компетентності, то це поняття є більше широким, інтегральним. Найчастіше його розглядають як: характеристику рівня професіоналізму особистості; спроможність кваліфіковано виконувати роботу; потенційну відповідність працівника вимогам. Це означає, що компетентним у певній сфері діяльності працівник стає не лише за наявності певного набору компетенцій, що визначають його потенційну відповідність вимогам, а лише в разі, коли рівень розвитку та прояву цих компетенцій досягає рівня, необхідного для професіонального виконання завдань. Отже, компетентність можна визначити як високий рівень опанування й активного використання компетенцій у професійній діяльності, що забезпечує досконале знання працівником сутності виконуваних завдань, уміння застосовувати дієві способи та заходи задля досягнення

намічених цілей, навички прийняття своєчасних раціональних рішень, керуючись власною інтуїцією, соціально-професійним досвідом. Відтак не компетенції працівника, а саме його компетентність у певній сфері професійної діяльності є передумовою успішної роботи в межах конкретної посади або організації в цілому (Л. Гуцан, 2013; К. Рудніцька, 2016).

Систематичні дослідження компетентнісного підходу в Україні було розпочато на початку 2000-х років, проте серед науковців досі немає єдиного розуміння його сутності, що наведено в табл.1.2.

Таблиця 1.2

Наукові підходи до трактування сутності компетентнісного підходу

Зміст поняття	Автор
«специфічна основа освітньої парадигми, фундамент її концепції, вказує на способи побудови тієї чи іншої освітньої системи»	О. Савченко, 2010
організація освітнього процесу з акцентом на формування та вдосконалення ключових (основних, базових) і предметних компетентностей, які необхідно засвоїти як учням, так і студентам у процесі навчання	В. Химинець
«переорієнтація з процесу на результат освіти в діяльнісному вимірі, забезпечення спроможності випускника відповідати новим запитам ринку, мати відповідний потенціал для практичного розв'язання життєвих проблем, пошуку свого «Я» у професії»	Н. Бібік, 2015
орієнтація освітнього процесу на формування й розвиток ключових, загальногалузевих і предметних компетентностей особистості	О. Пометун
«...наукова концепція, що має бути покладена в основу для визначення мети, змісту, методів та організації навчання, діагностики рівнів готовності і відповідності особистості до ефективної діяльності на відповідній посаді або у конкретній професійно-фаховій сфері»	В. Маслов та Л. Ващенко, 2010
метод організації освітнього процесу, який акцентує увагу на формуванні у людини необхідного обсягу знань і досвіду, що дозволяють їй аргументовано висловлювати свої думки, робити обґрунтовані висновки та діяти відповідно до обставин у різних життєвих ситуаціях	А. Хуторський
інструмент модернізації змісту освіти, що забезпечує його відповідність актуальним потребам сучасного суспільства	Н. Побірченко

Аналізуючи теоретичні дослідження, ми доходимо висновку, що компетентнісний підхід є невід'ємною частиною сучасної освіти, особливо в управлінській діяльності. Цей підхід дозволяє переосмислити цілі та зміст навчання, поставивши акцент на формуванні практичних навичок і здатності застосовувати знання на практиці. Такий підхід не лише підвищує якість підготовки фахівців, але й

готує їх до успішної професійної діяльності (Г. Єльнікова, 2010; О. Мармаза, 2017; В. Пержун, 2020).

Як свідчить рис. 1.1, успішне управління підприємством неможливе без урахування його стратегічного потенціалу, особливо людського, адже саме компетенції працівників, як внутрішній ресурс, визначають їхню готовність до ефективної роботи й успішність підприємства загалом. Тому застосування компетентнісного підходу в управлінні є ключовим для досягнення стійких результатів.

Метою нашого дослідження є глибоке розуміння компетентнісного підходу як інструменту управління, з акцентом на виявлення, розвиток та використання ключових компетенцій, які забезпечують конкурентоспроможність організації в динамічному середовищі (С. Леськова, 2023). Особливу увагу приділяють ролі ключових компетенцій у контексті управління закладом освіти. Отже, на початку ХХІ століття компетентнісний підхід став ключовим у системі управління закладом освіти та підготовки фахівців, як в Україні, так і на міжнародному рівні (Освітній менеджмент, 2003).



Рис. 1.1. Сутність компетентнісного підходу до управління підприємством (У. Гузар, Т. Гринчишин, 2018)

Застосування компетентнісного підходу відкриває широкі перспективи для розвитку людського потенціалу, оскільки сприяє формуванню ключових компетенцій, необхідних для успішної роботи в сучасному динамічному світі. Дослідження в цій галузі мають неабияке значення для підвищення конкурентоспроможності окремих фахівців і закладу в цілому.

1.2 Особливості реалізації компетентнісного підходу в освіті

Світові тенденції в освіті, зокрема в Україні, демонструють перехід до компетентнісного підходу, який має на меті підготувати молодь до викликів сучасного світу. Щоб здійснити управління на будь-якому рівні, сучасному менеджеру необхідно не просто опанувати набір знань, а й освоїти принципово новий підхід до навчання та виховання, який відповідатиме вимогам часу. Це потребує суттєвих змін у всіх складових системи освіти, а отже, і в самій системі як цілісній структурі, оскільки, формування в молоді комплексу компетенцій, необхідних для успішної професійної діяльності, адаптації до мінливих умов життя в сучасному світі XXI століття є актуальним та складним завданням освітньої політики (Л. Васильченко, 2006; Л. Тесленко, 2022). Загалом зміни мають відбутися в таких аспектах: цінності, цілі та результати освіти, зміст навчання, діяльність викладача й учня, а також у формах, методах і засобах навчання та виховання.

Інноваційні процеси в освіті здійснюються як цілісний комплекс змін у цілях, змісті, методах, формах та засобах діяльності, які характеризуються новизною, високою ефективністю, систематичністю та узгодженістю з іншими нововведеннями (О. Мармаза, 2016). Важливо також оновити освітнє середовище закладу і його взаємини із зовнішнім середовищем – сім'єю, суспільством, виробництвом, засобами масової інформації, державою, країною та світом. Освітня система намагається задовольнити ці запити шляхом упровадження компетентнісного підходу, який об'єктивно відповідає викликам сучасності. Динамічне середовище потребує фахівців, які вміють оперативно, гнучко реагувати на зміни, постійно навчатися, удосконалюватися, розвиватися. У доповіді ЮНЕСКО зазначено: «Усе частіше підприємці шукають у працівниках не просто кваліфікацію, яка часто асоціюється лише з технічними навичками виконання матеріальних операцій, а компетентність – своєрідний комплекс навичок, притаманний кожній людині. Цей комплекс поєднує професійну кваліфікацію в класичному сенсі, соціальні навички, вміння працювати в команді, ініціативність та схильність до ризику» (І. Петрова, Б. Остаєвський, 2023).

Сучасний заклад освіти вже за замовчуванням не може обмежуватися лише підготовкою кадрів – це загальносвітова тенденція, яку неможливо ігнорувати. Стратегічною метою освіти є формування компетентної особистості учня, здатної до самовизначення, самоосвіти, саморегуляції, самореалізації та успішної конкуренції на ринку праці. Також визнана потреба орієнтуватися на розвиток у випускників таких якостей, які забезпечать їм конкурентоспроможність на ринках праці (можливості працевлаштування) та здатність бути ефективними суб'єктами трудової діяльності впродовж усього життя (Н. Гузій, 2015).

Як зазначено в доповіді ЮНЕСКО «Освіта: прихований скарб», Ж. Делор виокремив чотири взаємопов'язані стовпи освіти, що охоплюють як інтелектуальний розвиток, так і соціальну й особистісну сфери: пізнання, діяльність, соціальну взаємодію та самореалізацію. Саме ці принципи лежать в основі глобальних компетентностей.

О. Крисан запропонував ієрархічну структуру класифікації компетентностей, яку М. Савчин зобразила у вигляді схеми, що дозволило детально проаналізувати складні взаємозв'язки між різними видами компетентностей (рис. 1.2.).



Рис. 1.2. Класифікація компетентностей

Визначений перелік ключових компетентностей, розроблений експертами АПН України, що були сформульовані на основі логічно визначеного порядку: вивчати – шукати – мислити – співпрацювати – діяти – адаптуватися, – охоплює як базові (уміння вчитися, комунікативна, соціальна), так і спеціалізовані (загальнокультурна, здоров’язбережувальна, громадянська, ІКТ) компетентності. Ключові компетентності – це багатокомпонентна структура, яка стосується освітніх стандартів і являє собою спеціально організований набір якостей особистості, що дозволяють ефективно функціонувати в будь-якому соціальному середовищі (рис. 1.3). Вони сприяють підвищенню якості суспільства, досягненню особистого успіху і допомагають у різних життєвих ситуаціях.

Ключові компетентності	
1	Вільне володіння державною мовою
2	Здатність спілкуватися рідною мовою
3	Здатність спілкуватися іноземними мовами
4	Математична компетентність
5	Компетентності в галузі природничих наук, техніки й технологій
6	Інноваційність
7	Інформаційно-комунікаційна компетентність
8	Екологічна компетентність
9	Навчання впродовж життя
10	Громадянські та соціальні компетентності
11	Культурна компетентність
12	Підприємливість і фінансова грамотність

Рис. 1.3. Ключові освітні компетентності

Ключові компетентності, за визначенням українських педагогів, – це загальні орієнтири, які конкретизуються у вигляді знань, умінь, навичок, цінностей і ставлень у межах різних навчальних предметів і життєвих ситуацій (рис. 1.4.). Ключові компетентності є наскрізними за своєю природою та мають бути сформовані під час навчання з використанням усіх предметів і виховних заходів без винятку.

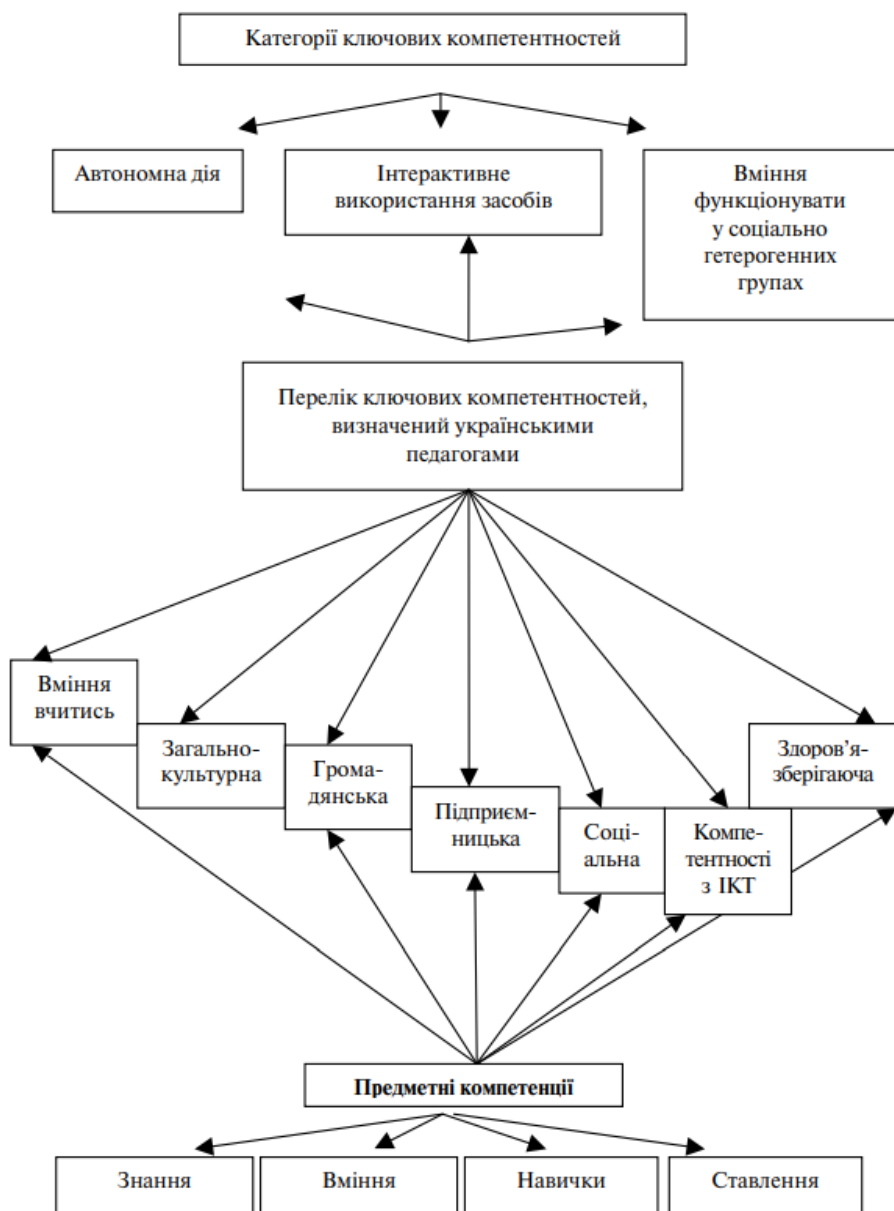


Рис. 1.4. Ключові компетентності (бачення українських педагогів)

Вивчаючи питання формування ключових компетентностей, І. Єрмаков узагальнює різні точки зору: «Щоб знайти своє місце в житті та успішно виконувати життєві й соціальні ролі, випускник української школи повинен володіти певними якостями та навичками»:

- бути гнучким, мобільним, конкурентоспроможним, здатним інтегруватися в динамічне суспільство та ефективно презентувати себе на ринку праці;
- застосовувати знання як інструмент для вирішення життєвих завдань;
- формувати нові ідеї, ухвалювати нестандартні рішення та відповідати за їх реалізацію;

- мати розвинену комунікативну культуру та вміти ефективно працювати в команді;
- вміти запобігати конфліктам та знаходити шляхи їх вирішення;
- знати, як отримувати та систематизувати інформацію з різних джерел і використовувати її для особистісного розвитку та самовдосконалення;
- дбайливо ставитися до власного здоров'я та здоров'я інших як найвищої цінності;
- мати здатність обирати з безлічі альтернатив ті, які пропонує сучасне життя (Л. Гуцан, 2013).

Реалізація компетентнісного підходу потребує радикального оновлення всіх компонентів освітньої системи. Згідно з класичною моделлю, освітній процес складається з таких кроків:

- формулювання мети;
- вибір змісту;
- визначення методів і форм роботи;
- вивчення результатів та перевірка їх відповідності поставленій меті;
- внесення змін до змісту.

Мотивація навчання пов'язана зі змістом освіти. Схему освітнього процесу можна представити таким чином (рис. 1.5.).

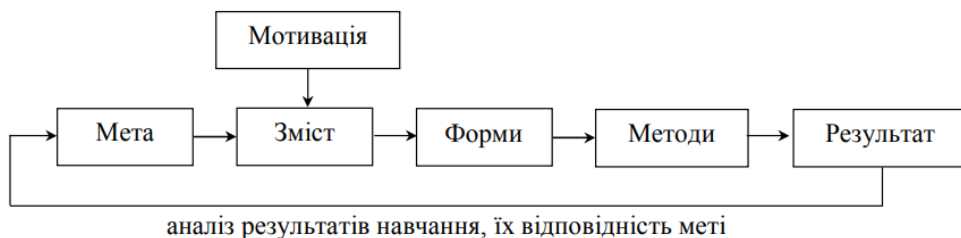


Рис. 1.5. Схема організації навчання за класичним зразком

У компетентнісному підході зміст освіти будується не навколо абстрактних цілей, а навколо конкретних результатів, яких учень має досягнути. На відміну від знань та вмінь, які можуть бути відсутні, компетентності завжди наявні в людини в певному вигляді, навіть якщо це мінімальний рівень. Цей початковий рівень є фундаментом для подальшого зростання. Тому в організації навчання за компетентнісним підходом важливо спочатку визначити, якими компетентностями здобувач освіти вже володіє, а потім будемо освітній процес, спираючись на цей рівень. Мотивація при цьому відіграє провідну роль на всьому шляху навчання за принципами компетентнісного підходу (рис. 1.6.).

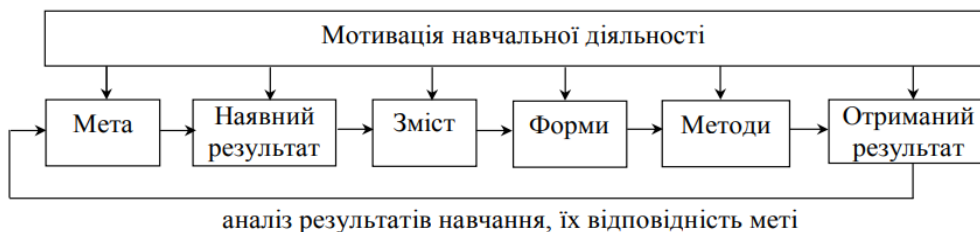


Рис. 1.6. Схема організації навчання, орієнтована на компетентнісний підхід

Упровадження загальної концепції компетентнісного підходу вимагає перегляду та переосмислення освітніх цілей (Н. Бібік, С. Бондар, Н. Голуб, О. Дахін, І. Єрмаков, В. Лозова, О. Локшина, А. Маркова, О. Мармаза, О. Овчарук, Л. Паращенко, О. Пометун, О. Савченко, Т. Хлебнікова та інші). Зміст Базового компонента дошкільної освіти та Державних стандартів освіти різних рівнів є компетентнісно спрямованим та ґрунтується на засадах особистісно зорієнтованого і компетентнісного підходів.

Головна мета освіти – це різнобічний розвиток здобувача освіти, розкриття його потенціалу та формування впевненої в собі особистості, готової до життя в сучасному світі. Компетентність розглядають як сукупність освітніх елементів, що проявляється у володінні системою знань, умінь і навичок, емоційно-ціннісними орієнтаціями, переконаннями особистості та готовності їх використовувати для пізнання навколишньої дійсності й задоволення власних потреб. Вона «формується в першу чергу на основі опанування змістом загальної середньої освіти», а «зміст шкільної освіти має бути аналогом соціального досвіду». Як зазначає І. Лернер, зміст освіти можна розглядати через призму таких складових:

- сукупність наукових знань як основи пізнання (когнітивна основа);
- комплекс практичних навичок (діяльнісний компонент);
- результати творчої діяльності, що відображають індивідуальний стиль і оригінальність (творча практика);
- комунікативний простір (сфера спілкування).

Ці складові змісту освіти повністю охоплюють усі необхідні компоненти основних складових компетентності (*Uri Peter Trier, 2001*). Порівняння попередніх і оновлених Державних стандартів свідчить про всебічний розвиток компетентнісної концепції (*О. Ісаєва, О. Єрченко, 2023*). О. Савченко підкреслює: «Якщо в попередньому стандарті ідею компетентнісного підходу було лише закладено, то в новому ми бачимо перехід до системної реалізації» (*О. Савченко, 2010*). Сучасний підхід до освіти виходить за рамки традиційного засвоєння знань. Державний стандарт вищої освіти зосереджений на розвитку не лише інтелектуальних, а й творчих та емоційних здібностей особистості. Крім знань та вмінь, він передбачає формування таких компетенцій, як здатність до самостійного мислення, творчості, критичного аналізу, а також емпатії та соціальної відповідальності. Закон України «Про вищу освіту» (2017) детально описує, яких результатів має досягти студент упродовж навчання, щоби бути готовим до викликів сучасного світу. На думку О. Савченко (2010), компетентнісний підхід передбачає поєднання таких компонентів, як знання, навички, уміння та особисті цінності, необхідні для адаптації до змін у соціальному середовищі. Основними принципами реалізації компетентнісного підходу є: 1) інтегративність змісту навчання. Компетентнісний підхід передбачає, що навчальний зміст має інтегрувати різні предметні галузі для формування цілісного сприйняття світу. В. Хомич підкреслює, що інтеграція знань допомагає краще застосовувати їх у реальних життєвих ситуаціях; 2) практична спрямованість навчання. Важливим аспектом є орієнтація навчання на практичне застосування здобутих знань. Наприклад, за словами Н. Виноградової, формування компетентностей потребує залучення учнів до вирішення реальних проблем і завдань; 3) особистісна орієнтованість. За Л. Ващенко, компетентнісний підхід враховує

індивідуальні особливості та потреби учнів, а також підтримує розвиток особистісної мотивації до навчання.

Фахівці Інституту педагогіки НАПН України провели комплексне наукове дослідження теоретичних засад традиційного та компетентнісного навчання. Результати дослідження дозволили чітко окреслити відмінності між цими двома підходами та сформулювати основні поняття компетентнісного підходу (рис. 1.7).

Традиційний підхід		Компетентнісний підхід
Формування всебічно розвиненої гармонійної особистості	Мета освіти	Формування діяльної компетентної особистості
Знання, вміння, навички	Основні освітні результати	Компетентність як готовність до успішної діяльності в різних сферах
Поступове формування спочатку знань, потім умінь та навичок	Особливості організації навчання	Інтеграція інтелектуальної та навичкової складових діяльності
Учитель: передає, навчає, формує. Переважає відтворення знань, застосування за зразком. Сам контроль і оцінює навчальні досягнення учнів	Методична реалізація. Позиція вчителя	Надає перевагу самостійній пошуковій діяльності учнів, проєктуванню навчальних і життєвих ситуацій для застосування предметних та ключових компетентностей; залучає дітей до самоконтролю, рефлексії
Підготовка учнів до найближчого майбутнього, яке є покращеною копією нинішнього життя	Формування інноваційного потенціалу школярів	Формування здатності жити в умовах постійних змін, бути ініціатором змін і активної соціальної дії
Розвиток інтелектуальної складової, відтворення знань («знання про всяк випадок»)	Способи використання знань	Формування навичок творчого використання знання як інструмента, засобу розв'язання проблем
Пріоритет соціального замовлення	Узгодження запитів суспільства та особистості	Пріоритет особистості, її замовлення на освіту
Зміст освіти формується «від мети»	Визначення змісту навчання	Зміст освіти формується «від результату»

Рис 1.7. Порівняння традиційного (знаннєвого) та компетентнісного підходів

Порівняльний аналіз виявив, що компетентнісний підхід не просто відрізняється від традиційного – знаннєвого, а є якісно новим підходом, який ставить за мету розвиток учнів як різнобічно розвинених особистостей, готових до життя в сучасному суспільстві. Цей підхід забезпечує більш високу ефективність навчання завдяки своїй спрямованості на розвиток практичних умінь, критичного мислення та творчих здібностей (В. Ягунов, 2013; К. Рудніцька, 2016).

Принципові відмінності компетентнісного підходу від традиційного (знаннєвого) такі:

- основний результат освіти полягає не лише в окремих знаннях, вміннях і навичках, а в здатності та готовності людини до ефективної діяльності в різних соціально важливих ситуаціях;
- поєднання інтелектуальної, навичкової та емоційно-ціннісної складової освіти;

- саморефлексія учнів щодо власних навчальних досягнень, усвідомлення своїх сильних і слабких сторін;
- формування у свідомості учня ціннісного ставлення до навчання як засобу самовдосконалення;
- використання гнучких підходів до оцінювання, що дозволяють виходити за рамки його традиційних норм.

Отже, реалізація компетентнісного підходу має такі особливості.

На рівні змісту освіти:

- відбір завдань має бути особистісно значущим для учнів;
- використання компетентнісних завдань, що не мають чітко визначених умов та вимагають пошуку нестандартних рішень;
- використання практико орієнтованих ситуацій, націлених на здобуття реального практичного досвіду, що мають соціальне значення.

На рівні організації освітнього процесу:

- переважання самостійної пізнавальної діяльності здобувачів освіти;
- створення умов для індивідуального розвитку кожного вихованця;
- можливість для учнів створювати власний освітній продукт;
- організація учнями презентації та захисту отриманих результатів;
- інтеграція інформаційних технологій в освітній процес;
- формування в учнів здатності до самооцінювання;
- диференційоване оцінювання кожного здобувача.

На рівні формування особистісних якостей:

- формування позитивної самооцінки, толерантності та емпатії на рівні загальнолюдських цінностей;
- розвиток навичок кооперації (співробітництва), а не конкуренції;
- розвиток уміння працювати в групі;
- заохочення до творчості й ініціативності.

Роль учителя в сучасному освітньому процесі зазнає кардинальних змін. Відповідно до компетентнісного підходу вчитель припиняє бути носієм готових знань, а стає організатором освітнього процесу, що стимулює активність і самостійність здобувачів. Створивши розвивальне освітнє середовище, учитель допомагає кожному учневі виявити свій потенціал і розвинути необхідні компетентності для успішного життя: критичне мислення, креативність, співпраця та самостійність. Упровадження компетентнісного підходу передбачає переосмислення освітніх результатів, переорієнтацію освітнього процесу й удосконалення механізмів його управління.

Сучасний етап розвитку освіти вимагає реалізації компетентнісного підходу на практиці, що зумовлює висування нових вимог до професійної діяльності педагогів. Це, зокрема, реалізується шляхом модернізації методичної роботи в закладах освіти й органах управління освітою. Оновлена система методичної роботи з педагогічними кадрами має бути зорієнтована на формування інноваційного стилю мислення та стійкої мотивації педагогів до самоосвіти і творчої діяльності. На нашу думку, найкращими способами виконання цього завдання є:

- забезпечення реальної та ефективної підтримки розвитку педагогічних працівників;

- забезпечення вектору змін – від знаннєвого підходу до діяльнісного, компетентнісного й особистісно орієнтованого адаптивного підходу щодо вибору форм роботи з кадрами;
- задоволення професійних інтересів педагогічних працівників, а також підтримка їх особистісного розвитку;
- формування інноваційного стилю мислення педагогів;
- створення умов для самовдосконалення та зацікавленості кожного вчителя в підвищенні кваліфікації та педагогічної майстерності;
- розширення різноманіття форм методичної роботи.

Оскільки активна свідома діяльність учасників освітнього процесу є основою компетентнісного підходу, використання діяльнісного підходу в методичній роботі, інтерактивних методів і залучення педагогів до активної участі в методичних заходах є цілком логічним. Упровадження концепції Нової української школи та нових Державних стандартів освіти вимагає кардинальних змін в освітній практиці. Компетентнісний підхід, який передбачає активне використання інноваційних технологій та орієнтацію на розвиток практичних навичок здобувачів, може стати рушійною силою цих змін. Однак для успішної реалізації компетентнісного підходу необхідні постійні дослідження, розроблення нових методів навчання та їх широке впровадження в освітній процес (О. Мармаза, 2015).

Глибокий аналіз компетентнісного підходу демонструє його тісний взаємозв'язок з ідеями педагогічної інноватики. Будь-яка сучасна інновація в освіті, спрямована на розвиток особистості учня та формування в нього практичних умінь і цінностей, є проявом компетентнісного підходу. Отже, компетентнісний підхід можна розглядати як системну інновацію, яка поєднує в собі ефективні досягнення педагогіки і відповідає вимогам сучасного суспільства.

Підсумовуючи все вищевикладене, виділяємо певні переваги та недоліки компетентнісного підходу, які необхідно враховувати під час його використання в управлінні закладами освіти (рис. 1.8.).

Переваги	Недоліки
<ol style="list-style-type: none"> 1. Інтеграція системи освіти країни у глобальний освітній простір 2. Забезпечує орієнтацію діяльності закладів освіти на вимоги роботодавців 3. Дозволяє орієнтуватись на забезпечення конкурентоспроможності фахівця 4. Забезпечує реалізацію комплексного та стратегічного підходів до розвитку освіти 5. Формує у молоді мотивацію до саморозвитку та самовдосконалення 	<ol style="list-style-type: none"> 1. Заклади освіти змушені поступитись фундаментальністю, оскільки у навчальних планах скорочуються базові дисципліни 2. Закріплення компетентностей в стандартах призведе до їх формалізації та обмежені можливостей до змін 3. Формулювання набору компетентностей не забезпечує їх автоматичну імплементацію в освітній процес 4. Значна кількість компетентностей, які вимагаються від фахівців, виходять за межі спроможності закладів освіти їх формувати 5. Досить складно визначити вичерпний перелік та зміст дисциплін, які формують ті чи інші компетентності

Рис. 1.8. Переваги та недоліки компетентнісного підходу

Реалізація компетентнісного підходу в українській освіті є багатограним процесом, який потребує системного аналізу та науково обґрунтованих рішень. Для досягнення успіху необхідно активізувати діяльність здобувачів освіти, орієнтувати освітній процес на розвиток практичних навичок і вмінь, забезпечити підвищення кваліфікації педагогів для системної реалізації компетентнісного підходу на практиці.

1.3 Управління закладом освіти на засадах компетентнісного підходу

В умовах євроінтеграції, глобалізаційних викликів сучасного суспільства, швидких змін у соціально-економічному, політичному житті країни важливе значення набуває освітній менеджмент як системостворювальний чинник якісних змін в організаційних засадах освітньої сфери, адже сучасний керівник має бути готовим до управління освітньою організацією в умовах реформування, забезпечувати ефективну взаємодію закладу освіти з державними установами та місцевими органами самоврядування, соціальними партнерами (*В. Святоха, 2013; А. Танько, 2019*).

Аналіз нормативно-правової бази України у сфері освіти дає змогу визначити ключові напрями трансформації освітнього менеджменту:

- цілеспрямована управлінська діяльність щодо створення безпечного освітнього середовища для всіх суб'єктів освітнього процесу;
- розвиток освітнього закладу на принципах інноваційності, конкурентоспроможності та демократичності;
- раціональне використання та розвиток кадрового потенціалу закладу освіти;
- створення й упровадження дієвої внутрішньої системи забезпечення якості освіти;
- управління закладом освіти з опорою на принципи партнерства й ефективної співпраці;
- адекватне забезпечення ресурсами для функціонування закладу освіти.

Необхідно відзначити, що розроблення нової моделі управління освітою, яка орієнтована на відкритість, демократію й розвиток самостійності, самодостатності та творчої активності особистості з метою зміцнення демократичних принципів громадянського суспільства, вимагає від сучасної освітньої системи значних реформаторських змін для вдосконалення управлінських механізмів.

Як зазначає В. Луговий, управління освітою – це процес цілеспрямованого впливу на її стан. Для досягнення високих показників в управлінні та забезпечення його результативності необхідно розуміти природу об'єкта управління, володіти актуальною інформацією для прийняття рішень, а також мати належні механізми та ресурси для їх реалізації (*В. Луговий, 2009*).

На думку О. Мармази, основною метою освітньої організації є формування особистості, яка є освіченою, креативною, фізично здоровою та всебічно розвинутою. Кінцевим результатом цього процесу є саме особистість. Така мета суттєво відрізняється від цілей підприємств чи комерційних установ, котрі орієнтуються на створення або розповсюдження матеріальних продуктів. Тому відповідальність за досягнення цілей та завдань в освітній сфері є значно складнішою та більш відповідальною. У ролі об'єктів управління виступають вчителі та інші працівники закладу, учні та їхні батьки, які є складними і багатограними через різноманітність

таких параметрів, як вік, соціальний статус, гендер та склад дитячого колективу (О. Мармаза, 2017).

Необхідно підкреслити, що в умовах реформування освітньої галузі суттєво змінюється і роль керівника закладу як лідера змін. Вивчення наукових джерел дає змогу виділити основні підходи до тлумачення цього поняття:

- це форма влади, яка характеризується напрямом зверху вниз і тим, що її носієм є не більшість, а окрема особа чи група осіб;
- це управлінська роль, соціальна позиція, що включає прийняття рішень, тобто керівна посада;
- це вплив на оточуючих.

У контексті багатовекторності трансформаційних процесів в освіті, вважаємо доцільним здійснити повний та всебічний аналіз компетентнісного підходу, оскільки він є втіленням інноваційного процесу освітньої системи, а компетентність виступає основним показником професіоналізму та готовності до виконання професійної діяльності. Тому поняття «ефективність освітнього менеджменту» пов'язують насамперед із компетентнісним підходом в управлінській діяльності. Основу компетентнісного підходу складають професійні стандарти. У межах професійного стандарту «Керівник (директор) закладу загальної середньої освіти», що охоплює два аспекти професійної діяльності: керівник-лідер і керівник-менеджер, – чітко визначені загальні та спеціалізовані компетенції, якими мають володіти керівники закладів. Серед ключових характеристик компетентнісного підходу в управлінні закладом освіти можна визначити кілька основних аспектів управлінської діяльності, а саме: ціннісне ставлення до інноваційного менеджменту як основного напрямку професійної діяльності, компетентність у забезпеченні якості освіти та функціонуванні внутрішньої системи управління якістю освітньої діяльності, а також здатність до професійного самовдосконалення (Г. Сльникова, 2010, 2017).

Компетентнісний підхід в управлінні закладом освіти полягає в здатності особистості виконувати складні, багатофункціональні, міждисциплінарні та культурно обґрунтовані види діяльності, ефективно виконуючи поставлені завдання. Компетентність охоплює володіння інструментами, що дозволяють людині ефективно організовувати як індивідуальну, так і колективну трудову діяльність. Отже, керівник закладу освіти повинен уміти ефективно керувати постійними змінами (О. Мармаза, 2016) та мати інноваційну позицію, яка включає такі компоненти: підтвердження професійної компетентності (яке має вплив на впровадження освітніх інновацій та формування іміджу закладу), зацікавленість у своїй діяльності, позитивне ставлення до нововведень та розуміння їхнього значення, а також упевненість у досягненні поставлених цілей.

Однією з важливих ознак компетентнісного управління, на думку науковців, є здатність керівника мотивувати та стимулювати педагогічний персонал до постійного професійного розвитку, сприяти гармонізації міжособистісних стосунків, об'єднувати педагогічний колектив, а також створювати ефективну систему професійно-педагогічної адаптації молодих спеціалістів до педагогічної діяльності (Л. Мартинець, 2016).

Згідно з компетентнісним підходом, ефективність виконання працівником своїх професійних обов'язків залежить від його здатності до практичного застосування

набутих компетенцій. Останнім часом компетентнісний підхід набуває все більшої популярності та намагається виконувати функцію концептуальної основи для ефективного функціонування управлінської системи і забезпечення загальної конкурентоспроможності корпорації. Відповідно до поглядів С. Прахалада та Г. Хамела, організацію необхідно розглядати як сукупність ключових компетенцій – навичок, умінь і технологій, що дають їй змогу формувати в споживачів певні цінності. Основним чинником успішного впровадження компетентнісного підходу є його орієнтація на комплексний розвиток компетенцій працівників, що включають знання, уміння, навички, досвід, здатність до адаптації, а також бажання до самовдосконалення і професійного зростання.

Компетентнісний підхід акцентує увагу не лише на знаннях і навичках особистості, а й на моделі професійної поведінки, що забезпечує прямий зв'язок між застосовуваними знаннями, уміннями та навичками з конкретними, вимірюваними результатами трудової діяльності працівника. Це дозволяє використовувати підхід у професійній діяльності (рис. 1.9), розуміти причини трудового успіху чи невдачі та вказує не лише на здатність людини виконувати необхідні професійні завдання, а й на відповідальність за їх виконання, усвідомлення способів досягнення бажаного результату.

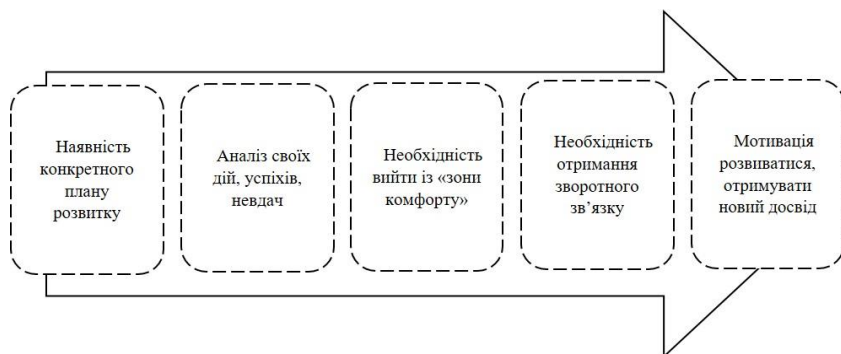


Рис. 1.9. Умови розвитку якостей, необхідних для впровадження в роботу компетентнісного підходу

Головне завдання компетентнісного підходу полягає в навчанні працівника ефективно керувати своїми знаннями, навичками й уміннями, тобто розвитку здатності до самонавчання та саморозвитку. Ще однією ключовою особливістю цього підходу є використання різноманітних характеристик компетенцій, що виявляються через поведінку, знання, навички та якості, що слугують підставами для оцінювання компетентності працівника. Крім того, ці характеристики демонструють конкретні ознаки професіоналізму працівника під час виконання своїх службових обов'язків (А. Вінченко, 2016).

Розроблення управлінських функцій з урахуванням компетентнісного підходу не лише допомагає втілювати стратегію розвитку освітнього закладу, а й сприяє розвитку самосвідомості та самокерування працівників, адже активна участь у процесах удосконалення діяльності закладу не може бути здійснена без участі працівників у самостійному пошуку та розширенні своїх знань і вдосконаленні індивідуальних здібностей.

Один із ключових аспектів компетентнісного підходу як концепції управління полягає в особливому підході до визначення її об'єкта. На відміну від знань і навичок працівників, які не завжди відповідають реальним потребам, ця концепція акцентує увагу на потенціалі співробітника – його здібностях, мотивації та поведінкових установках. Орієнтація на явні та приховані можливості працівників стимулює їх активну участь у діяльності організації, підвищує задоволеність працею та формує постійну потребу в удосконаленні знань, навичок і компетенцій (Л. Пшенична, 2020).

Сучасні заклади освіти дедалі частіше впроваджують ідеї компетентнісного підходу у всі сфери управління, при цьому модель компетенцій стає основним елементом системи, навколо якого концентруються конкретні функціональні напрямки управління. Можна стверджувати, що компетентнісний підхід є цілісною концепцією, яка визначає основні принципи управління в сучасних організаціях. Рівень кваліфікації та професіоналізму персоналу, його здатність ефективно виконувати завдання й генерувати прибуток безпосередньо залежать від тих теоретичних і практичних методів роботи з людьми, що застосовують менеджери організації у своїй щоденній практиці. Тому важливо забезпечити узгодженість між компетенціями працівників і організації, орієнтуючи їх на виконання завдань, що сприяють оптимізації управлінських процесів (рис.1.10).

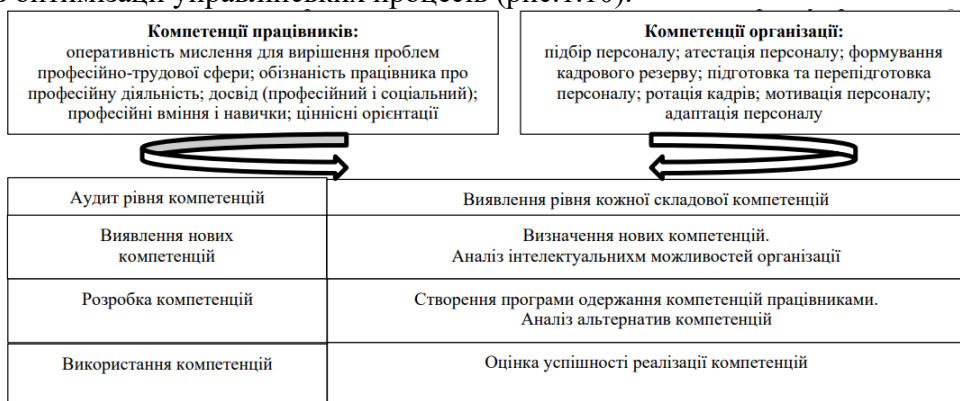


Рис. 1.10. Узгодженість між компетенціями працівників і організації в межах компетентнісного підходу до управління (У. Гузар, Т. Гринчишин, 2018)

Як було зазначено раніше, компетенції поєднують таланти та прагнення працівника й відображають його поведінку на виробництві. Це не просто знання, а і здатність застосовувати їх у професійній діяльності. Наприклад, до компетенцій можна віднести розв'язання управлінських проблем (збирання й аналізування інформації, виявлення проблем, розроблення альтернативних рішень і вибір стратегії дій), а також вплив на інших (поширення важливої інформації, подолання труднощів і супротиву, уміння визначати дії інших людей). Отже, компетенції набувають цінності не як самі по собі, а лише в тому випадку, коли вони допомагають працівникам досягати конкретних результатів відповідно до поставлених завдань. Врешті-решт, управління на основі компетентнісного підходу можна розглядати як необхідну умову для забезпечення конкурентоспроможності організації.

Слід підкреслити, що керівник закладу освіти є офіційно відповідальною особою за управління установою та організацію її функціонування. Зокрема, стаття

26 Закону України «Про освіту» (2017) визначає повноваження, надані керівнику закладу освіти. Отже, керівник закладу загальної середньої освіти має низку обов'язків щодо управління діяльністю ЗЗСО, включаючи фінансові, господарські, адміністративні та інші аспекти, а також забезпечення якості освітнього процесу та створення сприятливих умов для навчання й викладання. Для реалізації концепції школи та досягнення поставлених цілей керівник активно працює в таких сферах, як стратегічне планування, педагогічна і дидактична діяльність, кадрова політика, а також моніторинг і оцінювання. Крім того, керівник акцентує увагу на взаємозв'язку між різними видами діяльності та сферами (О. Касьянова, 2013):

- зовнішні фактори розвитку та внутрішні ресурси, які сприяють втіленню бачення або концепції ЗЗСО;
- уявлення про майбутнє та його стратегічні завдання;
- завдання та конкретні напрямки діяльності;
- напрями діяльності в одній сфері (освітнє лідерство) та напрямки в інших сферах (підтримка команди і супервізія).

Ми також поділяємо думку колег-науковців, які розглядали основні вимоги до професійної підготовки сучасних керівників у сфері освіти, розподіливши їх на дві основні групи – професійні й особистісні. Професійна складова охоплює загальнопрофесійну та управлінську компетентність, тоді як особистісна складається із соціальних і професійно важливих якостей. Підкреслено, що ці компоненти тісно взаємопов'язані, отже, спроби формувати професійну компетентність без розвитку особистісних якостей фахівця є малоефективними (Д. Смоліч, 2021).

Л. Сігасва та А. Опольська відзначають важливість розвитку в керівників таких компетентностей, які в певному сенсі відповідають вимогам Національної рамки кваліфікацій та ініціативи ЄС Тюнінг:

- інтегральна компетентність – це здатність виконувати складні завдання та проблеми в управлінській діяльності або в процесі навчання, яка також включає проведення досліджень й упровадження нововведень і має ознаки непостійності умов та вимог;

- загальні компетентності включають в себе здатність до абстрактного мислення, аналізу, синтезу та визначення взаємозв'язків між соціально-економічними процесами; уміння застосовувати теоретичні і базові знання, розуміти специфіку професії менеджера та її предметну область; навички роботи з інформаційно-цифровими технологіями для збирання, оброблення, аналізування й використання даних із різних джерел; здатність ефективно працювати в команді та налагоджувати міжособистісну взаємодію під час виконання професійних обов'язків; бажання постійно навчатися та здобувати нові знання; уміння адаптуватися, проявляти креативність, генерувати нові ідеї та знаходити рішення в незнайомих ситуаціях;

- фахові компетентності включають здатність ефективно керувати організацією та її підрозділами, реалізуючи функції менеджменту; уміння аналізувати результати діяльності освітньої установи, порівнювати їх із чинниками, що впливають ззовні та зсередини організації, визначати можливості для її розвитку; уміння обирати й застосовувати сучасні інструменти управління; здатність до

ефективного планування та організації часу; уміння оцінювати та забезпечувати високу якість виконуваних завдань; здатність формувати та організовувати продуктивні комунікації в процесі управління; здатність аналізувати та розв'язувати проблеми організації, приймати обґрунтовані рішення; уміння управляти змінами; розуміння принципів права та їх застосування у професійній діяльності; знання психологічних принципів і здатність використовувати їх для досягнення ефективності в роботі.

М. Смирнова, досліджуючи специфіку виконання управлінських функцій керівника Нової української школи, виділяє традиційні управлінські дії, що характерні для директора ЗЗСО:

- управління діяльністю закладу;
- створення умов, що сприяють продуктивній діяльності вчителів і учнів, а також моніторинг діяльності всіх підрозділів закладу освіти;
- покращення й оновлення матеріально-технічної інфраструктури закладу, створення позитивного іміджу та розвитку організаційної культури школи.

Зазначені дії відображають управлінський функціональний цикл, який включає етапи планування, організації, мотивації та контролю (за М. Альбертом, М. Месконом і Ф. Хедоурі).

Із упровадженням Концепції «Нова українська школа» функції директора ЗЗСО перебувають у процесі суттєвих змін, що пов'язані з новими викликами, акцентами в управлінській діяльності та орієнтацією на потреби сучасного соціокультурного та освітнього середовища, а також з очікуваннями учасників освітнього процесу. М. Смирнова підкреслює, що в управлінській діяльності директора Нової української школи особливу роль відіграють мотиваційно-ціннісні орієнтири, лідерська позиція керівника та його емоційна компетентність.

В. Ткаченко зазначає, що на етапі реформування освітньої системи сучасний керівник повинен мати низку компетенцій і вмінь:

- зосереджуватися не лише на досягнутих результатах, а й на самому процесі та взаємодії;
- шукати оптимальний рівень участі членів колективу в процесі прийняття рішень;
- сприяти ефективному виконанню поставлених завдань;
- сприяти формуванню мотивувального уявлення про майбутнє та вміння передавати його іншим членам команди;
- бути інноваційним лідером і наставником;
- сприяти діалогічному підходу в спілкуванні з учнями та педагогічним колективом (В. Ткаченко, 2017).

Сучасні дослідники також пропонують розглядати управління освітніми закладами в межах парадигми лідерства. Дж. Коллінз зазначає, що для того, щоби стати лідером, керівник має пройти через кілька послідовних етапів: висококваліфікований працівник, цінний член команди, компетентний менеджер, ефективний керівник та лідер (Л. Даниленко, Л. Карамушка, 2003).

За словами Г. Єльнікової, термін «культура управлінської праці» охоплює різні аспекти культури, зокрема загальну (або загальнолюдську), політичну,

правову, естетичну, педагогічну, а також їх різноманітні варіації, що визначаються типом і особливостями конкретного освітнього закладу (Г. Єльнікова, 2017).

Дослідники виділяють ключові вимоги до керівника закладу освіти, які включають його професійні знання та навички, позитивний досвід педагогічної діяльності, а також певні особистісні та професійні якості. До таких якостей належать: організованість, здатність до ефективної комунікації, переконливість, рішучість, відповідальність, впевненість у своїх силах, креативність, висока моральність, толерантність, чуйність, гуманність, доброта, справедливість, комунікабельність, оптимізм та прагнення до самовдосконалення (О. Гречаник, В. Григораши, 2019; О. Касьянова, 2015; М. Ксенофонтowa, Т. Заболотна, 2012).

До основних професійних знань можна віднести розуміння сучасних теорій і моделей управління освітою, інноваційних технологій, стилів керівництва, методів покращення ефективності управлінської діяльності та якості освітніх послуг, а також основних принципів менеджменту в освітніх установах.

До професійних умінь можна віднести встановлення ефективних ділових контактів, організацію та планування діяльності закладу, управління конфліктними ситуаціями, делегування завдань, створення умов для всебічного розвитку педагогічного колективу та учнів, прийняття управлінських рішень та інші. Важливим аспектом є взаємозв'язок між професійними і особистісними якостями керівника освітньої установи.

Отже, основними компонентами цієї схеми є професійні та особистісні якості керівника, що визначають його здатність ефективно застосовувати свої знання та навички, які реалізуються через функції професійної діяльності. Під функціями професійної діяльності керівника закладу освіти розуміються окремі напрями керівництва, які повинні підтримуватись відповідними управлінськими діями. Основними функціями управління є: організація, планування, координація, прогнозування, прийняття і реалізація управлінських рішень, регулювання та коригування діяльності закладу, стимулювання та мотивація педагогічного процесу, а також контроль і корекція освітнього процесу.

Розуміння терміну «професійна компетентність» є ключовим для розвитку професійних навичок менеджера у сфері освіти. У межах функціонально-діяльнісного підходу професійну компетентність можна трактувати як поєднання теоретичних знань і практичної готовності керівника до виконання своїх обов'язків. Поняття «професійна компетентність» включає рівень освіти, досвід, особисті здібності, мотивацію до безперервного навчання та самовдосконалення, а також творчий і відповідальний підхід до виконання завдань. До ключових характеристик професіоналізму керівника ЗЗСО відносять:

- знання й усвідомлення сутності управлінської діяльності та процесів менеджменту;
- знання посадових і функціональних обов'язків керівника в освіті, а також професійну відповідальність;
- здатність ефективно застосовувати інформаційно-цифрові технології й інші інструменти комунікації, важливі для управлінської діяльності;
- здатність до професійної рефлексії, розуміння людських аспектів та уміння

ефективно встановлювати як зовнішні, так і внутрішні зв'язки.

Отже, професійну компетентність керівника ЗЗСО можна описати як сукупність знань, навичок та досвіду, які необхідні для ефективного виконання його посадових обов'язків і досягнення результативності в діяльності закладу освіти (В. Крамчанін, 2021).

Л. Даниленко та Л. Карамушка розглядають професійну компетентність керівника закладу освіти як комплекс необхідних для ефективної діяльності знань і навичок, що охоплюють науково-філософські, суспільно-політичні, психолого-педагогічні, предметні та соціально-функціональні аспекти, а також відповідні особистісні риси. Згідно з думкою авторів, професійна компетентність керівника включає такі компоненти:

- необхідні знання, що стосуються педагогічної спеціалізації або конкретної посади;
- здібності та навички, що є важливими для ефективного виконання функціональних та посадових обов'язків;
- професійні, ділові й особистісні характеристики, що сприяють повному використанню потенціалу, здібностей і можливостей у процесі виконання функціональних і посадових обов'язків;
- загальна культура, важлива для розвитку гуманістичного світогляду, визначення духовних і ціннісних орієнтирів, а також формування моральних і етичних принципів особистості;
- стимул до професійної діяльності (Л. Даниленко, Л. Карамушка, 2003).

В. Маслов трактує професійну компетентність керівника закладу освіти як сукупність теоретичних і методологічних основ, нормативних принципів, наукових знань, організаційно-методичних і технологічних навичок, що необхідні для виконання посадових обов'язків, а також відповідних моральних і психологічних характеристик особистості (В. Маслов, 2010).

О. Курило, Л. Савко та О. Солянік, аналізуючи компетентність керівника як ключовий фактор удосконалення управлінського процесу, пов'язують її з такими аспектами, як професіоналізм, ефективність управлінської діяльності, розв'язання управлінських завдань, а також підкреслюють її особистісний характер.

П. Олешко вважає, що професійна компетентність керівника закладу освіти є важливим показником його готовності до управлінської діяльності та здатності приймати ефективні управлінські рішення, акцентуючи увагу на її інтегративному характері.

Дослідники здебільшого аналізують питання управління на основі компетентнісного підходу через призму менеджменту, при цьому завдання розвитку професійних компетентностей особистості визначають як основний пріоритет (Інновації в управлінні закладами освіти, 2021).

Т. Сорочан визначає зміст професіоналізму управлінської діяльності керівника закладу освіти з огляду на сукупність таких компетенцій:

- функціональна компетентність охоплює здатність відновлювати традиційний управлінський цикл школи та володіти здібностями виконання управлінських обов'язків;

- соціально-педагогічна компетентність полягає в ефективному управлінні школою як складною соціальною системою;
- соціально-економічна компетентність передбачає ефективне управління школою в умовах ринкової економіки, а також володіння принципами менеджменту та маркетингу в освітній сфері;
- інноваційна компетентність полягає в орієнтації на вдосконалення педагогічної системи школи на основі впровадження новітніх інновацій;
- фасилітативна компетентність полягає в орієнтації на підтримку творчої роботи педагогічного колективу для формування унікальних освітніх практик (Т. Сорочан, 2003).

На нашу думку, упровадження компетентнісного підходу є важливим на всіх етапах управління освітою, зокрема для управлінських кадрів. Їх слід не лише навчати, а й постійно стимулювати до ініціативи та професійного розвитку, використовуючи різноманітні методи мотивації до творчості та інновацій. Ключовим є забезпечення ефективної координації з науковими та методичними установами, а також оновлений науково-методичний супровід діяльності педагогічних працівників. Завдання сучасного керівника не обмежується прийняттям рішень, він створює сприятливі умови для їх реалізації: зібрати команду однодумців, організувати ефективну систему комунікації між усіма учасниками освітнього процесу, забезпечити постійний моніторинг на всіх етапах, мотивувати й контролювати впровадження інновацій, дотримувати норм охорони праці та знаходити способи покращення матеріально-технічної бази. Важливо, щоб кожне управлінське рішення наближало заклад до основної мети – забезпечення здобувачам якісної освіти, результатом якої стане компетентний випускник, здатний реалізувати свої життєві плани й бути успішним.

Отже, успіх сучасного закладу освіти безпосередньо пов'язаний із лідерськими якостями його керівника. Саме від професіоналізму й умінь адаптуватися до змін залежить, чи зможе заклад освіти трансформуватися та відповідати викликам часу. Керівник є каталізатором розвитку, який не лише виконує повсякденні завдання, а й визначає стратегічний напрямок руху закладу.

Підсумовуючи сказане вище, зазначимо, що аналіз теоретичних засад компетентнісного підходу дозволив визначити основні етапи його розвитку.

Компетентнісний підхід передбачає спрямування освіти на досягнення результатів, що включають формування загальнокультурних і професійних компетенцій, підтримку самовизначення, соціалізації, індивідуального розвитку та реалізації особистісного потенціалу. Цей підхід націлює освітню систему на забезпечення якості підготовки, що відповідає сучасним соціальним запитам. Він одночасно враховує потребу особистості в інтеграції до суспільного життя і вимогу суспільства ефективно використовувати її можливості та таланти.

Було розглянуто особливості реалізації компетентнісного підходу в освіті. Порівняно традиційний (знансвий) і компетентнісний підходи, виокремили їх принципові відмінності. Науково-теоретичні дослідження дали змогу виділити певні переваги та недоліки компетентнісного підходу, які необхідно враховувати під час його впровадження.

Ми поділяємо точку зору науковців, які вважають що управління освітою – це процес цілеспрямованого впливу на її стан. Основною метою освітньої організації є формування особистості, яка є освіченою, креативною, фізично здоровою й різнобічно розвинутою. Аналіз основних аспектів управління закладом освіти на засадах компетентнісного підходу дає можливість дійти висновку, що розуміння терміну «професійна компетентність» є ключовим для розвитку професійних навичок менеджера у сфері зокрема загальної середньої освіти. Отже, керівник закладу освіти повинен уміти ефективно керувати постійними змінами та мати інноваційну позицію.

2. Практика вдосконалення управління закладом освіти на засадах компетентнісного підходу

2.1. Аналіз стану управління закладом освіти на засадах компетентнісного підходу

Базою нашого практичного дослідження було обрано КЗ «Харківська гімназія № 92 Харківської міської ради», що розташована в Новобаварському районі м. Харкова.

Нами було складено програму аналізу, відповідно до якої експертна група, сформована з числа фахівців управління освіти та ХГ № 92, здійснила оцінювання.

Мікродослідження № 1. Оцінювання рівня управлінської компетентності керівника (за кваліметричною моделлю).

Мета: визначити параметри та фактори, які потребують покращення й розвитку.

Як було зазначено в теоретичному розділі, управлінська компетентність, включає когнітивний, операційний і особистісний компоненти. Ми визначили ці елементи як параметри моделі. Для оцінювання параметрів використано методи аналізу документації ЗЗСО, протоколи атестації керівника на час його призначення на посаду, опитування та спостереження. Результати оцінювання наведені в таблиці 2.1. Для проведення оцінювання нами використано кваліметричну модель, розроблену В. Григорашем (2019).

Таблиця 2.1

Рівень професійної компетентності керівника ЗЗСО

Параметри	К_{ваг.}	Фактори	К_{ваг.}	Оцінка
1. Когнітивний компонент K=0,68	0,3	Законодавчо-нормативні знання	0,3	0,7
		Загальнотеоретичні знання (менеджмент, психологія, педагогіка, фінанси, економіка, соціологія, право, філософія)	0,3	0,6
		Методологічні знання (дошкільної педагогіки, психології, навчання дорослих, окремих методик, технології і методика аналізу і контролю, технологія планування діяльності, знання методів управління організацією, закономірностей розвитку колективу, методика наукових досліджень)	0,4	0,9

2. Операційний компонент К= 0,7	0,4	Діагностичні вміння (аналіз, діагностика, моніторинг)	0,1	0,6
		Прогностичні вміння (прогнозування, визначення стратегічних цілей, управління маркетингом)	0,2	0,6
		Організаційні вміння (організація інструктивно-регулятивної діяльності, управління інноваційною діяльністю, організація взаємодії із зовнішнім середовищем, батьками, громадськістю, організація державно-громадського управління, самоврядування, координація й узгодження діяльності структурних підрозділів, посадових осіб)	0,3	0,7
		Аудиторські вміння (проведення внутрішнього аудиту ЗЗСО)	0,3	0,7
		Інформаційна компетентність	0,1	0,7
3. Особистісний компонент К= 0,71	0,3	Мотивація досягнення успіху, соціально спрямована орієнтація особистості	0,1	0,9
		Сформованість досвіду емоційно-ціннісних відносин, особистісних ставлень і орієнтацій	0,1	0,9
		Комунікативна культура, здатність до аргументованого дискусування, сформованість комунікативних навичок (встановлення контакту, комунікативна ініціатива, культура мовлення)	0,2	0,8
		Креативність, здатність до творчої діяльності, інноваційної діяльності, науково-дослідницької роботи	0,2	0,7

К = 0,7 – достатній рівень.

З огляду на результати дослідження, можна стверджувати, що керівник має достатній рівень управлінської компетентності. Потребують удосконалення діагностичні та прогностичні вміння керівника ЗЗСО.

Також нами досліджено компетентність директора гімназії за показниками, розробленими Департаментом освіти для атестації керівника.

Мікродослідження № 2. Рівень управління ЗЗСО.

Мета: визначити рівень управління ЗЗСО як показник професійної компетентності керівника закладу.

Результати оцінювання, форми й методи збирання інформації представлено в таблиці 2.2.

Таблиця 2.2

Рівень управління гімназією

№ з/п	Критерії	Показники діяльності ЗЗСО, питання, що підлягають аналізу	Форми і методи збору інформації	Рівень освітньої діяльності			
				Високий	Достатній	Середній	Низький
1.	Програма розвитку закладу освіти, планування його діяльності відповідно до вимог законодавства	- програма розвитку ЗЗСО; - відповідність планів роботи на навчальний рік та оздоровчий період завданням загальної середньої освіти	Б Д		9		
2.	Внутрішній аудит, аналіз усіх напрямів діяльності ЗЗСО та звітування	- щоденник внутрішнього аудиту; - матеріали щорічного звітування керівника закладу	Б Д			6	
3.	Ведення ділової документації	відповідність ведення ділової документації вимогам нормативно-правових актів	Д	10			
4.	Організація роботи щодо виявлення, підтримки та розвитку обдарованості, природних нахилів і здібностей дітей	організація діяльності ЗЗСО за пріоритетними напрямками	С Д			4	
5.	Діяльність педагогічної ради	- склад педагогічної ради; - кількість засідань, що проводять на рік; - тематика засідань; - рішення, що ухвалюють; - наявність наказів керівника на виконання рішень педагогічної ради;	С Д				3

		- стан контролю за виконанням рішень педагогічної ради					
6.	Громадський рейтинг ЗЗСО	Сз – кількість скарг громадян щодо діяльності ЗЗСО, які надійшли до його керівництва, органів управління освітою (за останні три роки); Св – кількість скарг, на які відповіли, розв'язали. – сайт ЗЗСО, своєчасність його оновлення	А Б Д С			6	
7.	Організація роботи з батьками	- Наявність інформаційного куточка для батьків у кожному класі, своєчасність його оновлення; - проведення заходів за участю батьків, їх періодичність, відповідність плану роботи; - план і періодичність роботи консультпункту	Д Б С	10			
8.	Дотримання вимог безпеки життєдіяльності та охорони праці працівників і учнів (за 3 останні роки)	С _{тр} – кількість випадків виробничого травматизму; У – середнє арифметичне загальної кількості дітей та працівників; – організація роботи з охорони праці	Д Б С		7		
9.	Аналіз і ліквідація зауважень під час інституційного аудиту (перевірки тощо)	- Програма (план) з усунення прогалин відповідає таким вимогам: повнота, конкретність, реальність встановлення строків виконання та визначення відповідальних тощо; - стан виконання вищезазначеного плану заходів. <i>За відсутності – 12 балів</i>	А Б Д С		9		

А – анкетування;

Б – бесіда;

Д – аналіз документації;

С – спостереження.

Спосіб визначення: експертна оцінка.

Формула для обрахунку:

$$C_3 = C_{3.1} + C_{3.2} + C_{3.3} + 2 * C_{3.4} + C_{3.5} + C_{3.6} + C_{3.7} + C_{3.8} + 2 * C_{3.9} + C_{3.10}$$

Загальна оцінка = 85 балів – достатній рівень.

Потребують удосконалення:

- система роботи з безпеки життєдіяльності й охорони праці;
- діяльність педагогічної ради;
- аналіз діяльності ЗЗСО;
- громадський рейтинг ЗЗСО.

Мікродослідження № 3. Творчий потенціал педагогічного колективу.

Мета: оцінювання рівня творчого потенціалу педагогів ЗЗСО.

Творча компетентність педагога посідає одне з провідних місць у його професійній компетентності, відтак актуально оцінити рівень розвитку творчого потенціалу педагогів.

Для оцінювання рівня творчого потенціалу педагогів ЗЗСО базового закладу освіти було проведено тестування «Ваш творчий потенціал» (додаток А), що дозволило визначити рівень творчого потенціалу педагогічних працівників.

Результати дослідження були обчислені за формулою:
 $K = \text{Загальна кількість балів} / 15.$

Графічний аналіз представлений у вигляді діаграми (рис. 2.1).

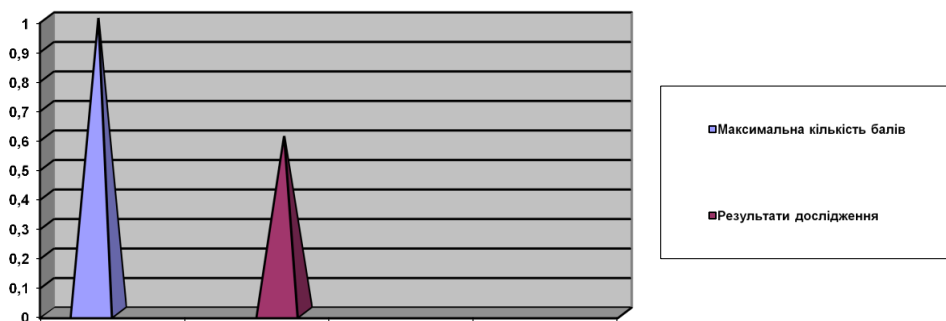


Рис. 2.1. Творчий потенціал педагогічного колективу

Аналіз результатів дослідження засвідчив, що педагогічний колектив гімназії № 92 має середній рівень творчого потенціалу. Варто зазначити, що вчителі потребують підтримки в організації освітнього процесу на основі принципів педагогіки партнерства, використання соціально-емоційного та етичного навчання, що сприятиме розвитку творчої індивідуальності як педагога, так і здобувача освіти.

Мікродослідження № 4. Управління розвитком творчої компетентності педагогів.

Мета: оцінити якість управлінської діяльності щодо розвитку творчої компетентності педагогів та визначити рівень управлінської діяльності в цьому напрямі.

Згідно з метою дослідження, було розроблено кваліметричну модель (додаток Б) для оцінювання якості управлінської діяльності з розвитку творчої компетентності педагогів (далі – ТКП) на основі досліджень О. Гречаник, В. Григораша, Г. Дмитренка, Г. Єльнікової, О. Касьянової, З. Рябової. Ми визначили сім факторів, які складають структуру кваліметричної моделі: інформаційне забезпечення управління розвитком творчої компетентності педагогів, науковість роботи з розвитку ТКП, розподіл управлінської праці між членами адміністрації з питань розвитку ТКП, організація особистої праці керівників з проблеми дослідження, забезпечення раціональної праці підлеглих із розвитку ТКП, створення умов для розвитку ТКП та результативність роботи за цим напрямом. Кожен із цих факторів містить критерії, які визначають показники. Також нами було запропоновано технологію оцінювання за моделлю та відповідні шкали, за якими встановлюють рівень управління. Для цього ми скористалися доробками науковців. Оцінку управління РТК педагогів визначають як суму всіх факторів. Узагальнену експертну оцінку графічно зображено на рис. 2.2.

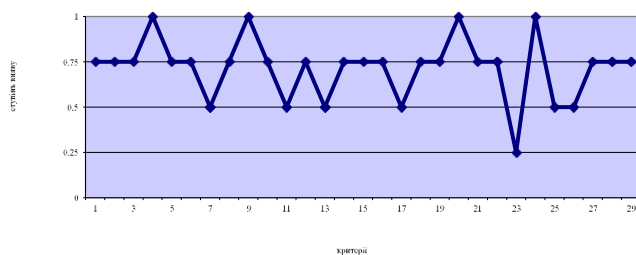


Рис. 2.2. Узагальнена експертна оцінка критеріїв за кваліметричною моделлю
Розрахунки за кваліметричною моделлю представлено в таблиці 2.3.

Таблиця 2.3

1. Результати розрахунків за кваліметричною моделлю

№ з/п	Коефіцієнт відповідності критерію K_i	Вагомість критерію V_i	Оцінка критерію $V_i K_i$	Σ критеріїв Φ_i	Вагомість фактору m_i	Оцінка фактору Φ_i
1.	$K1=0,75$ $K2=0,75$ $K3=0,75$	0,3 0,2 0,5	0,225 0,15 0,375	0,75	0,12	$\Phi1=0,09$
2.	$K4=1$ $K5=0,75$ $K6=0,75$	0,25 0,5 0,25	0,25 0,375 0,1875	0,81	0,15	$\Phi2=0,12$
3.	$K7=0,5$ $K8=0,75$ $K9=1$ $K10=0,75$	0,4 0,1 0,2 0,3	0,2 0,075 0,2 0,225	0,7	0,14	$\Phi3=0,1$
4.	$K11=0,5$ $K12=0,75$ $K13=0,5$ $K14=0,75$	0,6 0,05 0,2 0,15	0,3 0,04 0,1 0,11	0,55	0,15	$\Phi4=0,08$

5.	K15=0,75 K16=0,75 K17=0,5	0,3 0,2 0,5	0,225 0,15 0,25	0,625	0,13	Φ5=0,08
6.	K18=0,75 K19=0,75 K20=1 K21=0,75 K22=0,75	0,15 0,15 0,3 0,2 0,2	0,11 0,11 0,3 0,14 0,14	0,8	0,14	Φ6=0,11
7.	K23=0,25 K24=1 K25=0,5 K26=0,5 K27=0,75 K28=0,75 K29=0,75	0,2 0,09 0,075 0,075 0,06 0,2 0,225	0,05 0,09 0,0375 0,0375 0,045 0,15 0,15	0,56	0,17	Φ7=0,1
Загальна оцінка якості управління РТК педагогів				О заг. = Φ1 + Φ2 + Φ3 + Φ4 + Φ5 + Φ6 + Φ7 = 0,68		
Рівень управління РТК педагогів				Допустимий		

Отже, аналіз стану управління ЗЗСО з позицій компетентнісного підходу дозволив виявити певні проблеми, які пропонуємо розв'язати завдяки розробленню й реалізації цільового проєкту.

2.2. Цільовий проєкт з удосконалення управління закладом освіти на засадах компетентнісного підходу та його експертиза

Глобалізація, інформаційна революція, утвердження ринкових відносин та загальна демократизація, відкритість кордонів і прозорість суспільного життя, міграція та активна взаємодія культур докорінно змінюють реальність. Водночас ці процеси несуть із собою виклики: масовізацію життєвого простору, поширення прагматичного мислення, глобальну нівеляцію духовно-моральних цінностей, таких як благородство, справедливість і милосердя. Серед інших проблем особливо актуальним стає питання виховання і навчання дітей у мінливих умовах сучасного світу.

Діти перебувають під значним впливом оточення, але бувають ситуації, коли педагог стає головним, а інколи єдиним духовним наставником для дитини. Це підкреслює потребу в сучасних професійних педагогах, здатних сприяти гармонійному розвитку особистості. Рівень духовності дитини багато в чому залежить від духовної культури дорослих – педагогів і батьків. Учитель має бути прикладом сердечності та доброти у взаєминах з учнями, допомагаючи формувати соціально значущі цінності та сенс життя молодого покоління.

Ці питання є важливими на державному рівні й закріплені у нормативних документах. Зокрема, Закон України «Про освіту» визначає освіту як фундамент інтелектуального, культурного, духовного, соціального й економічного розвитку суспільства та держави. В Україні освіта визнана пріоритетною сферою розвитку, а її основні принципи – гуманізм, демократизм, пріоритет загальнонародських духовних

цінностей, а також нерозривний зв'язок із національною та світовою історією, культурою й традиціями.

Як зазначено в Національній доктрині розвитку освіти, сучасна освіта покликана сприяти формуванню нової, цілісної суспільної системи. Вона має бути відкритою, багатоманітною, наповненою духовними та культурними цінностями, толерантною, здатною виховувати громадянина й патріота та об'єднувати суспільство навколо пріоритету прав особистості.

Для реалізації цілей державної освітньої політики необхідно, щоб професійна підготовка педагогів відповідала сучасним викликам суспільства. Учитель має не лише досконало володіти своїм предметом, але й бути майстром педагогічної діяльності, а також носієм високої духовної культури.

Проблема збагачення духовного рівня педагогів і підвищення їхньої професійної майстерності є однією з ключових у нинішніх умовах розвитку суспільства. Сучасна школа потребує вчителя, здатного не лише оновлювати й удосконалювати свою діяльність, але й бути прикладом високих моральних принципів і духовної культури.

Тому освітні установи мають приділяти більше уваги формуванню духовної культури педагога-професіонала. Зокрема, у процесі науково-методичної роботи акцент слід робити на розвиток духовності вчителя, що стане основою для підвищення його професійної компетентності та майстерності (*О. Перехейда, 2012*).

Основна ідея проєкту полягає в розвитку професійної компетентності вчителя, його компетенцій, духовної культури, що дозволяє йому не лише дбати про збереження здоров'я здобувачів та забезпечувати їхню безпеку, але й вводити їх у світ краси, добра, прищеплювати цінності національної та світової культури, виховувати основи духовної культури. Це вимагає нового підходу до управління розвитком професійної компетентності педагогів. Духовну культуру вчителя розглядаємо як поєднання високої професійної підготовки та багатого духовного світу особистості.

Сучасний педагог має володіти передовими педагогічними технологіями, з любов'ю і повагою ставитися до своєї професії та демонструвати високий рівень духовної культури, яка є основою його професійної майстерності.

Мета проєкту: розроблення й упровадження інноваційної моделі збагачення духовної культури педагога, яка стане базою для підвищення професійної компетентності вчителів, зокрема шляхом інтеграції цієї моделі в освітній процес гімназії.

Завдання проєкту:

1) визначення сутності та структури духовної культури педагога: дослідження основних аспектів духовної культури та специфіки її розвитку в умовах освітнього процесу гімназії;

2) проєктування та експериментальна перевірка: створення та апробація змісту, форм і методів організації науково-методичної роботи з педагогами, спрямованої на розвиток їхньої духовної культури;

3) вивчення й розроблення умов для використання педагогічних технологій: аналіз і впровадження педагогічних технологій, які сприяють удосконаленню духовності педагогів гімназії, що є основою підвищення їхньої педагогічної майстерності;

4) створення умов для самовираження педагогів: забезпечення можливостей для реалізації індивідуальних здібностей педагогів, розвитку їхнього прагнення до професійного самовдосконалення і підвищення рівня духовної культури;

5) визначення критеріїв ефективності: розроблення критеріїв оцінювання ефективності організації науково-методичної роботи в гімназії щодо розвитку духовної культури педагогів як бази для підвищення їхньої професійної компетентності;

6) розроблення методичних рекомендацій: підготовка рекомендацій для вдосконалення організації науково-методичної роботи в напрямі розвитку духовної культури педагогів.

Концептуальні засади проєкту:

1) культура:

- система цінностей, яка необхідна для творчого та активного осмислення світу;

- вона є фундаментом формування як особистості, так і культури суспільства загалом;

- культура слугує основою освітнього процесу;

2) духовна культура:

- сукупність моральних норм, звичаїв, обрядів, вірувань, які формувалися впродовж громадсько-історичної діяльності;

- є ключовим елементом для виховання особистості та розвитку педагогічної компетентності;

3) педагогічна компетентність:

- вираження творчої активності педагога;

- найвищий рівень професійної діяльності вчителя, що реалізується через процес його самореалізації;

4) культура як основа педагогічної майстерності:

- виконує роль духовного камертона та світоглядної основи для творчого підходу в педагогічній діяльності;

- є джерелом унікальності, нестандартних рішень та креативності вчителя;

5) учитель:

- носій високих духовних і загальнокультурних цінностей;

- посередник між культурою суспільства та учнем, який сприяє передачі й засвоєнню культурних надбань.

Ці концептуальні положення забезпечують основу для створення інноваційного підходу до розвитку педагогів, що гармонійно поєднує професійну майстерність із духовними й культурними цінностями.

Специфіка проєкту:

проєкт спрямований на організацію дослідно-експериментальної роботи в умовах освітнього процесу гімназії з метою створення інноваційної моделі розвитку духовної культури педагогів як основи їхньої професійної компетентності. Аналіз засвідчив, що вчителі гімназії мають високий творчий потенціал, потребу в інноваційній діяльності, а також виявляють значний інтерес до здобуття нових знань і освоєння сучасних педагогічних технологій. У реалізації проєкту беруть участь представники науки, мистецтва, громадських організацій, викладачі закладів вищої

освіти, учителі гімназії, здобувачі освіти та їхні батьки. Ця співпраця забезпечує інтеграцію теоретичних знань, творчих підходів і практичних навичок, сприяючи гармонійному розвитку духовної культури педагогів і учнів.

Очікувані результати проєкту для адміністративної ланки гімназії передбачають низку значущих змін. Одним із головних досягнень стане підвищення культури освітнього менеджменту, що дозволить вдосконалити управлінські процеси. Адміністрація зможе опанувати стратегію управління, засновану на людиноцентристських підходах, гуманістичних традиціях і інноваційних підходах до організації освітнього процесу. Також передбачено освоєння технології моніторингу процесу формування ключових компетентностей і духовної культури педагогів, що сприятиме оцінюванню ефективності запропонованих змін. Важливим результатом стане впровадження механізмів і прийомів стимулювання педагогів до інноваційної діяльності, що забезпечить підвищення якості освіти та мотивацію до професійного зростання.

Очікувані результати для педагогів включають зростання зацікавленості у своїй професії, що сприятиме підвищенню мотивації до професійного розвитку. Учителі опанують методiku самостійної діяльності, технології саморозвитку та самовиховання, що допоможе їм у постійному вдосконаленні. Важливим досягненням стане засвоєння методів педагогічної підтримки та підвищення рівня духовної культури, які дозволять створювати більше гармонійні стосунки зі здобувачами освіти. У процесі реалізації проєкту педагоги опанують інноваційні технології, зокрема змістовно-пошукові, особистісно-розвивальні, компетентісно зорієнтовані підходи до навчання та виховання, а також технології життєтворчості особистості. Це дозволить їм розробляти власні ефективні педагогічні методики. Водночас відбудеться їхнє кваліфікаційне зростання, підвищення професійної компетентності та вдосконалення навичок гуманного, партисипативного й духовного стилю спілкування. Учителі навчатимуться надавати індивідуальну педагогічну підтримку, конструктивно розв'язувати конфлікти та суперечності, що сприятиме формуванню позитивного освітнього середовища й підвищенню ефективності їхньої роботи.

Очікувані результати для здобувачів освіти: здобувачі покращать свої навчальні досягнення, а також сформують духовну культуру та розвинуть інтелектуальні, моральні та соціальні якості. Важливим аспектом є вдосконалення ціннісних орієнтирів, емоційної сфери, творчих здібностей та особистісних рис кожного учня. Крім того, будуть створені умови для самореалізації учнів, усвідомленню ними свого місця в гімназії. У процесі навчання учні здобудуть навички дослідницької та проєктної діяльності.

Очікувані результати для батьків: підвищення рівня психолого-педагогічної освіти та розвитку духовної культури, а також налагодження і зміцнення дружніх стосунків між родинами вихованців і закладом освіти.

Очікувані результати для громадськості: підвищення уваги й інтересу до питань виховання духовної культури в гімназії, а також активна участь у розв'язуванні проблем освіти.

Термін реалізації: один рік.

Етапи реалізації проєкту

1. Аналітико-концептуальний етап.

1.1. Заснування науково-методичного центру для координації проєкту.

- 1.2. Аналіз нормативно-правових документів.
- 1.3. Дослідження теоретичних та методологічних аспектів, опрацювання літературних джерел.
- 1.4. Обговорення концепції та плану впровадження проєкту.
- 1.5. Підготовка необхідної документації.
- 1.6. Формування груп для проходження тренінгів.
- 1.7. Розрахунок витрат на реалізацію проєкту.
2. *Організаційно-методичний етап.*
 - 2.1. Розроблення моделі моніторингу виконання проєкту.
 - 2.2. Створення комплексу діагностичних методик.
 - 2.3. Проведення методологічного семінару для педагогів щодо практичного впровадження проєкту.
 - 2.4. Діагностика рівня мотиваційної та технологічної готовності педагогів до професійного розвитку.
 - 2.5. Організація психологічної підтримки педагогічного колективу.
 - 2.6. Пошук та аналіз необхідної інформації.
3. *Практичний етап.*
 - 3.1. Реалізація запланованих заходів проєкту.
 - 3.2. Опанування педагогами сучасних освітніх технологій, орієнтованих на демократизацію взаємодії.
 - 3.3. Упровадження інноваційних методів навчання, спрямованих на особистісний розвиток і компетентнісний підхід.
 - 3.4. Оптимізація системи управління освітнім закладом із гуманістичним спрямуванням.
 - 3.5. Комплексний моніторинг рівня духовної культури педагогів.
 - 3.6. Розроблення цілісної інноваційної моделі формування духовної культури для підвищення професійної майстерності.
4. *Рефлексивно-результативний етап.*
 - 4.1. Оцінювання досягнутих результатів.
 - 4.2. Узагальнення отриманих даних.
 - 4.3. Обговорення результатів проєкту з колективом та громадськістю у форматі круглого столу.
 - 4.4. Презентація підсумків роботи.
 - 4.5. Визначення подальших напрямів розвитку проєкту.
 - 4.6. Проведення науково-практичної конференції «Компетентнісне управління освітою: досвід, результати, перспективи».
 - 4.7. Підготовка методичних матеріалів для публікації.

**План
роботи ХГ № 92 ХМР щодо реалізації проєкту**

№ з/п	Зміст діяльності	Термін виконання	Відповідальний	Контроль
2. Адміністративно-організаційні заходи				

1.1	Організувати науково-методичний координаційний центр, що забезпечуватиме загальне керівництво проєктною діяльністю	Серпень, 2025 р.	Директор гімназії	
1.2	Створити інформаційний (у тому числі комп'ютерний) банк даних про інноваційні технології підвищення професійної майстерності й духовної культури педагогів	Вересень, 2025 р.	Заступник директора з науково-методичної роботи	
1.3	Створити банк даних, що міститиме перспективний педагогічний досвід гімназії, району, міста, України, досягнення вітчизняних і зарубіжних учених та практиків, а також інформацію про нові надходження до бібліотеки	Серпень-вересень, 2025 р.	Заступник директора з науково-методичної роботи, зав. кафедрами, бібліотекар	
1.4	Оцінити та визначити рівень мотиваційної готовності педагогів гімназії до впровадження проєкту	Вересень, 2025 р.	Заступник директора з науково-методичної роботи, психолог	
1.5	Скласти прогноз та визначити основні чинники опору змінам серед педагогічного колективу гімназії	Жовтень, 2025 р.	Психолого-акмеологічна служба	
1.6	Оновити нормативно-правову основу (накази, розпорядження, рекомендації тощо) для впровадження інновацій у межах реалізації проєкту	Вересень-жовтень, 2025 р.	Науково-методична рада	
1.7	Оновити чинну нормативно-правову базу гімназії (статут, правила внутрішнього трудового розпорядку, режим роботи) відповідно до потреб реалізації проєкту, узгодити зміни з внутрішніми органами управління гімназії та забезпечити їхнє подальше затвердження	Вересень, 2025 р.	Рада гімназії, директор	

1.8	Обговорити теоретичну модель проєкту з підвищення управлінської та професійної компетентності, духовної культури педагога на засіданнях: <ul style="list-style-type: none"> • предметних кафедр; • науково-методичної ради; • педагогічної ради 	Серпень, 2025 р. Серпень, 2025 р. Серпень, 2025 р.	Зав. кафедрами Заступник директора з науково-методичної роботи Директор гімназії	
1.9	Розробити стратегію управлінської взаємодії між усіма учасниками проєкту	Серпень, 2025 р.	Директор гімназії	
1.10	Окреслити та сформулювати функціональні обов'язки науково-методичної ради гімназії та предметних кафедр, а також розширити їхні повноваження у контексті реалізації проєкту	Вересень, 2025 р.	Заступник директора з науково-методичної роботи, зав. предметними кафедрами	
1.11	Забезпечити взаємодію культурно-просвітницьких установ, що знаходяться на території Новобаварського району м. Харкова	Вересень-жовтень, 2025 р.	Учитель образотворчого мистецтва	
1.12	Упорядкувати банк інформаційно-цифрових технологій	Серпень, 2025 р.	Директор гімназії	
3. Науково-методичне й управлінське забезпечення розвитку професійної майстерності і духовної культури педагогів				
2.1	Науково-методична тема гімназії спрямована на розв'язання проблем, пов'язаних із підвищенням професійної компетентності вчителів засобами науково-методичної роботи, удосконаленням професійної компетентності кожного вчителя, розвитку їх творчої ініціативи; упровадженням в	Протягом року	Науково-методична рада	

	освітній процес досягнень перспективного педагогічного досвіду, інноваційних проєктів, новітніх технологій та забезпеченням їх практичної реалізації; забезпеченням реалізації принципів гуманізації, демократизації та спрямованістю процесу навчання на розвиток особистості здобувача освіти; активізацією видавничої діяльності вчителів та участю в інноваційній та дослідно-експериментальній роботі; підвищенням інформаційно-цифрової компетентності педагогів			
2.2	Розширення функцій предметних кафедр у напрямку підвищення професійної майстерності та духовної культури педагогів. Коригування організації роботи кафедр гімназії та уточнення їхнього статусу	Упродовж року	Адміністрація гімназії	
2.3	Оновлення структури науково-методичної ради гімназії, визначення її юридичного статусу та підрозділів: – науково-методичний координаційний центр для експериментальної роботи; – інформаційно-ресурсний відділ; – психолого-функціональна служба; – лабораторія моніторингових досліджень якості освіти	Вересень, 2025 р.	Адміністрація гімназії	
2.4	Провести засідання науково-методичної ради, обговорити такі питання: 1. Духовна культура як складова професіоналізму вчителя.	Серпень, 2025 р.	Заступник директора з	

	2. Управління розвитком духовної культури особистості вчителя засобами науково-методичної роботи	Лютий, 2026 р.	науково-методичної роботи	
2.5	Провести засідання педагогічної ради, обговорити такі питання: 1. Взаємозв'язок духовної культури вчителя та учнів в умовах сучасного соціокультурного розвитку суспільства. 2. Самовдосконалення педагога як чинник розвитку його духовної культури та професійної позиції	Жовтень, 2025 р. Березень, 2026 р.	Заступник директора з виховної роботи Заступник директора з навчально-виховної роботи	
2.6	Запровадити серію вебінарів і майстерок щодо розвитку професійної майстерності класного керівника	Щокварталь но	Заступник директора з виховної роботи	
2.7	Організувати роботу науково-теоретичного семінару на тему: «Духовна культура педагога й керівника освіти»	Щомісячн о	Заступник директора з науково-методичної роботи	
2.8	Створити електронний банк курсів підвищення кваліфікації педагогічних працівників	Січень, 2025 р.	Науково-методична рада	
2.9	Розробити програму підвищення кваліфікації цифрової компетентності педагогічних працівників	Жовтень, 2025 р.	Науково-методична рада	
2.10	Сприяти проходженню педагогами та керівниками гімназії курсів підвищення кваліфікації за окремо складеним планом	Червень, 2026 р.	Директор гімназії	
2.11	Організувати функціонування батьківського клубу «Виховання духовної культури дитини»	Протягом року	Заступник директора з виховної роботи	

2.12	Розробити комплексне методичне забезпечення курсів з основ етики, психології, філософії та світової художньої культури	Травень 2026 р.	Завідувачі предметних кафедр, учителі	
2.13	Забезпечити участь педагогічних працівників і здобувачів освіти у науково-практичній конференції «Розвиток системи управління організацією: Європейська практика та досвід України»	Щотравня	Зав. кафедрами, наукове товариство гімназистів	
2.14	Організувати науково-методичні консультації, співбесіди, а також індивідуальні та групові бесіди з учителями щодо організації пошуково-дослідницької та експериментальної діяльності	Упродовж року	Зав. предметних кафедр	
2.15	Залучити учнів до написання творчих робіт для захисту на засіданнях МАН з тематики	Упродовж року	Керівники кафедр	
2.16	Оновити освітні програми, розробити навчальні програми предметів «Етика», «Педагогіка» тощо	Квітень-травень, 2026 р.	Вчителі-предметники	
2.17	Розробити план проведення предметних тижнів для здобувачів освіти	Щорічно	Зав. предметних кафедр	
2.18	Організувати воркшоп «Розвиток креативного мислення» для педагогів і вихованців	Протягом року	Науково-методична рада	
2.19	Продовжити традицію проведення науково-практичних читань для вчителів, метою яких є збагачення колективного педагогічного досвіду через впровадження інновацій	Березень, 2026 р.	Заступник директора з науково-методичної роботи	
3. Соціально-психологічний супровід проєктної діяльності				
3.1	Удосконалити структуру функціонально-психологічної служби, визначити її статус	Серпень, 2025 р.	Директор гімназії, практичний психолог	

3.2	Провести діагностику та здійснити аналіз психологічної готовності вчителів гімназії до реалізації проекту	Вересень, 2025 р.	Практичний психолог	
3.3	Провести психолого-педагогічний консиліум «Саморозвиток духовності особистості»	Квітень, 2026 р.	Практичний психолог	
3.4	Організувати роботу постійно-діючого психолого-педагогічного семінару «Психологія гуманістичної складової духовності»	Щомісячн о	Практичний психолог	
3.5	Організувати й провести психологічні тренінги й тренінги особистісного росту педагогів	Упродовж року	Практичний психолог	
3.6	Створити банк даних про стан розвитку креативних та комунікативних здібностей учителів	Упродовж року	Практичний психолог	
3.7	Розробити механізми соціальної підтримки вчителів	Листопад, 2026 р.	Профспілковий комітет, дирекція гімназії	

4. Організація співпраці із закладами вищої освіти

4.1	Розробити пакет нормативно-правових документів про роботу з вищими навчальними закладами	Серпень, 2025 р.	Дирекція гімназії, науково-методична рада	
4.2	Модернізувати договірні стосунки з вищими навчальними закладами	Упродовж року	Дирекція гімназії	
4.3	Розробити й апробувати наскрізні сумісні програми з ХНПУ імені Г. С. Сковороди з культурології, філософії, основ правознавства	Упродовж року	Предметні кафедри	
4.4	Створити й організувати наукові товариства учнів на базі кафедр ЗВО	Упродовж року	Заступник директора з навчально-виховної роботи	
4.5	Залучити викладачів вищих навчальних закладів до	Упродовж року	Науково-методична рада	

	проведення курсів, семінарів з питань професійного росту педагогів та збагачення їх духовної культури			
4.6	Вивчити можливості введення спеціальних інтегрованих курсів та викладання їх силами викладачів вузів	Протягом року	Заступник директора з науково-методичної роботи	
4.7	Продовжити співпрацю та урізноманітнити форми співробітництва з ХНПУ імені Г. С. Сковороди, ХНУ імені М. Каразіна	Упродовж року	Директор гімназії	
5. Мотивація і стимулювання розвитку професійної компетентності педагогічних працівників				
5.1	Всебічно сприяти самоствердженню вчителя у колективі, підвищенню його педагогічної майстерності й духовної культури	Упродовж року	Адміністрація, профспілки	
5.2	Створити умови для вивчення досвіду роботи кращих шкіл міста Харкова, України	Упродовж року	Заступник директора з науково-методичної роботи	
5.3	Забезпечити стажування вчителів гімназії на базі Харківського ліцею № 89 (за угодою)	Червень, 2026 р.	Зав. предметними кафедрами	
5.4	Провести громадський огляд надбань перспективного педагогічного досвіду	Березень, 2026 р.	Атестаційна комісія гімназії	
5.5	Організувати й провести творчий звіт кафедри естетичного циклу	Грудень, 2025 р.	Зав. кафедрою	
5.6	Провести декаду наставника та ініціативи й творчості молодих вчителів	Січень, 2026 р.	Науково-методична рада	
5.7	Забезпечити участь педагогів у різноманітних конкурсах педагогічної майстерності, зокрема «Учитель року»	Грудень, 2025 р.	Заступник директора з науково-методичної роботи	

5.8	Продовжити практику ведення «Книги пошани майстрів педагогічної справи»	Упродовж року	Науково-методична рада	
5.9	Провести церемонію вручення професійних нагород, відзначення досягнень учителів у визначених номінаціях	Травень, 2026 р.	Дирекція гімназії, профспілковий комітет	
5.10	Забезпечити розробку педагогами авторських програм професійно-особистісного саморозвитку й портфоліо	Протягом року	Заступник директора з науково-методичної роботи	
5.11	Практикувати використання атестаційної процедури для стимулювання підвищення професійної майстерності й духовної культури педагогів	Протягом року	Атестаційна комісія	
5.12	Залучити досвідчених педагогів гімназії до навчально-методичної та дослідницької роботи в статусі співробітників відповідних кафедр КВНЗ «ХАНО» (на громадських засадах)	Протягом року	Зав. предметними кафедрами	
5.13	Удосконалити систему матеріального заохочення педагогічних працівників	Жовтень, 2025 р.	Рада гімназії, директор	
5.14	Практикувати висвітлення педагогічного досвіду вчителів гімназії на сторінках фахових видань, у соціальних мережах	Протягом року	Науково-методична рада	
6. Ресурсне забезпечення проєкту				
6.1	Поповнити фонд бібліотеки, методичного кабінету, медіатеки необхідними матеріалами для професійного росту вчителів	Упродовж року	Бібліотекар	
6.2	Підготувати матеріали за результатами проєкту для публікації в спеціальному випуску науково-педагогічного журналу «Харківський колегіум»	Грудень, 2026 р.	Рада гімназії, науково-методична рада	

6.3	Забезпечити опис і тиражування досвіду роботи учителів у фахових виданнях	Упродовж року	Адміністрація	
6.4	Створити й забезпечити функціонування сайту проєкту	Протягом року	Методист з інформаційних технологій	
6.5	Підготувати до друку науково-методичний посібник «Педагогічна інноватика»	Серпень, 2026 р.	Директор гімназії, науково-методична рада	
7. Моніторинг проєктної діяльності				
7.1	Розробити пакет діагностичних методик для різних етапів проєктної діяльності	Протягом року	Науково-методична рада, лабораторія моніторингових досліджень	
7.2	Запровадити індивідуальну методичну картку з метою моніторингу динаміки професійного росту педагогів	Вересень, 2025 р.	Заступник директора з науково-методичної роботи	
7.3	Організувати презентацію портфоліо	Березень, 2026 р.	Науково-методична рада	
7.4	Розробити алгоритм корекції самоосвітньої діяльності вчителів під час реалізації проєкту	Грудень, 2025 р.	Лабораторія моніторингових досліджень	
7.5	Удосконалити засоби вимірювань і технологію проведення моніторингу проф. компетентності вчителя	Травень, 2026 р.	Лабораторія моніторингових досліджень	
8. Управління упровадженням проєкту				
8.1	Створити інформаційну систему управління реалізацією проєкту й встановити порядок користування цією системою	Вересень, 2025 р.	Директор гімназії	
8.2	Організувати аналіз ходу реалізації проєкту в гімназії	Протягом року	Рада гімназії, директор	
8.3	Провести поточний і підсумковий аналіз реалізації проєкту	Щоквартально	Заступник директора	
8.4	Організувати планування процесу розробки й реалізації проєкту (стратегічних, тактичних планів і планів поточної діяльності)	Серпень, 2026 р.	Директор гімназії, науково-методична рада	

8.5	Розробити плани організації і реалізації проєкту (розроблення навчальних планів, програм, планів введення інновацій). Спланувати відкриття нових видів освітніх послуг для модернізації освітньої системи гімназії	Серпень, 2026 р.	Директор, науково-методична рада	
8.6	Контролювати хід планування процесу розробки й реалізації проєкту	Вересень, 2025 р.	Директор гімназії	
8.7	Узгодити план реалізації проєкту з іншими планами і програмами гімназії	Вересень, 2025 р.	Заступник директора	
8.8	Проводити моніторинг виконання планів реалізації проєкту, його поточними й підсумковими результатами, заслуховувати звіти учасників проєкту, виявляти недоліки й вносити зміни у процес його реалізації	Протягом року	Директор гімназії	
8.9	Контролювати процес реалізації системи заходів інформаційного, кадрового, організаційного, науково-методичного, нормативно-правового, матеріально-технічного та фінансового забезпечення реалізації проєкту	Протягом року	Директор гімназії	
9. Фінансове забезпечення проєкту				
9.1	Спланувати фінансування реалізації проєкту: визначення бюджету по статті заробітної плати, навчання, матеріально-технічних і науково-методичних засобів і стимулювання роботи	Серпень, 2025 р.	Директор гімназії	
9.2	Відшукати джерела й укласти угоди з питань фінансування проєкту	Протягом року	Директор гімназії, гол. бухгалтер УО	
9.3	Організувати контроль за витратою засобів, відпущених на реалізацію проєкту	Протягом року	Директор гімназії	

Після розроблення цільового проєкту він повинен пройти експертну оцінку для визначення прогнозованої якості. Для цього була створена експертна група з 12 осіб, до складу якої увійшли керівники, психолог і педагоги ХГ № 92, а також директорки ЗЗСО № 28, 39, 59, 127, 153. Було розроблено план роботи експертної групи, який включав: визначення мети та завдань, розподіл повноважень, з'ясування критеріїв оцінювання, безпосереднє проведення експертного оцінювання, узагальнення та оформлення результатів, а також розроблення методичних рекомендацій для впровадження проєкту.

Для експертизи цільового проєкту члени експертної групи адаптували критерії, запропоновані О. Мармазою (2015):

- актуальність – відповідність сучасним і майбутнім освітнім проблемам;
- системність – взаємодія всіх основних компонентів проєкту: мети, завдань, змісту діяльності, можливість моніторингу програми;
- реалістичність – відповідність наявним і прогнозованим ресурсам.
- повнота – врахування комплексу проблем і завдань, що постають перед ЗЗСО, охоплення всіх учасників ОП;
- психологічний супровід – співробітництво і гласність у діях, забезпеченість психодіагностичними вимірюваннями, сприятливий мікроклімат;
- продуктивність – вплив на систему знань, умінь, навичок керівників ЗЗСО, педагогів, здобувачів освіти та їхніх батьків;
- наукова новизна – ступінь новизни в діяльності учасників ОП;
- оптимальність – урахування можливостей ЗЗСО та учасників ОП;
- рефлексивність – можливість самоаналізу діяльності учасників ОП;
- особистісна результативність – динаміка управлінської компетентності керівника, ТКП і здобувачів освіти.

Експерти виставляли оцінки від 0 (повна відсутність критерію) до 5 балів (максимальний прояв критерію). Оцінку проєкту обраховували за формулою:

$$K = \left(\frac{1}{10} \right) \left(\sum_{i=1}^{10} K_i \right), K \leq 1, \quad (1)$$

Результати оцінювання проєкту експертами представлено на рис. 2.3, 2.4.

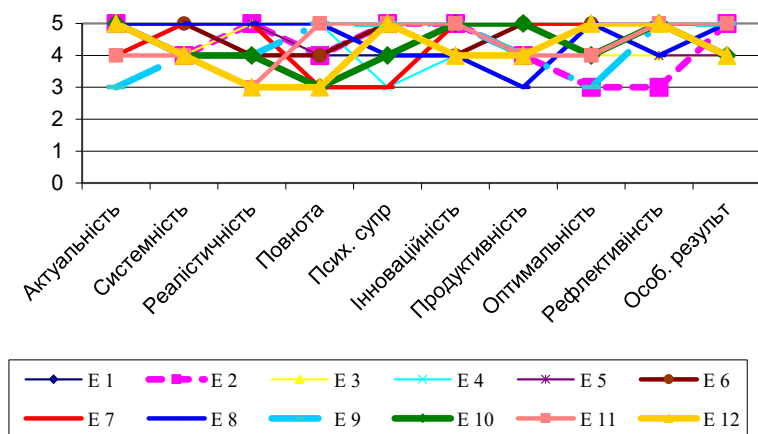


Рис. 2.3. Результати оцінювання цільового проєкту за критеріями

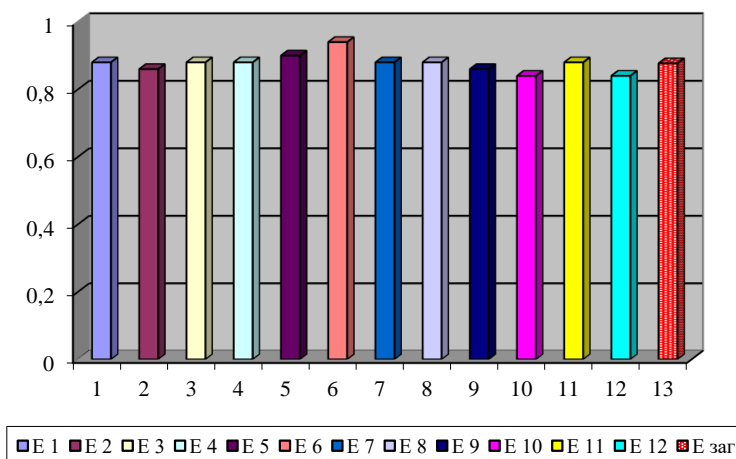


Рис. 2.4. Загальна експертна оцінка проєкту й оцінки, виставлені експертами

Як показують дані рис. 2.3, 2.4, загальна експертна оцінка цільового проєкту становить 0,877, що відповідає достатньому рівню. Відтак розроблений проєкт з удосконалення управління закладом освіти на засадах компетентнісного підходу отримав схвалення експертної групи і був запропонований для впровадження в практику роботи ЗЗСО протягом 2025-2026 рр. за умов наявності належного фінансування.

Отже, вивчення практики вдосконалення управління закладом освіти на засадах компетентнісного підходу дозволили дійти таких висновків.

Було впорядковано й частково розроблено діагностичний інструментарій, складено програму дослідження, сформовано експертну групу.

Рівень управлінської компетентності керівника базового закладу освіти – достатній (оцінка 0,7).

Рівень управління закладом загальної середньої освіти – достатній.

Рівень розвитку творчого потенціалу педагогічного колективу – середній.

Рівень управління розвитком творчої компетентності педагогів – допустимий (оцінка 0,68).

Для вдосконалення управлінської діяльності було обрано розроблення цільового проєкту. Ми обґрунтували актуальність проєкту, визначили його мету та завдання, сформулювали концептуальні засади і окреслили етапи впровадження: діагностико-концептуальний, організаційно-теоретичний, практичний та підсумково-презентаційний. Також був розроблений план реалізації заходів проєкту на один рік.

Для проведення експертної оцінки розробленого проєкту визначено 12 критеріїв та відповідні їм показники: актуальність, системність, реалістичність, повнота, психологічний супровід, інноваційність, продуктивність, оптимальність, рефлексивність та особистісна результативність. Експертна група з 12 осіб здійснила оцінку проєкту, результат – 0,877, рівень – достатній. Проєкт був рекомендований експертною групою до впровадження за умов наявності фінансових ресурсів.

Основним висновком дослідження є досягнення мети та окреслених у вступі завдань, проте отримані результати не є вичерпними. Уважаємо перспективним напрямом у цьому контексті визначення інструментів і методик для ефективного формування компетентностей здобувачів.

References:

- Бібік Н. Переваги і ризики запровадження компетентнісного підходу в шкільній освіті. *Український педагогічний журнал*. 2015. № 1. С. 47-58. URL: <https://surl.lu/vpuhdi> (дата звернення: 08.02.2025).
- Варецька О. В. Розвиток соціальної компетентності вчителя початкової школи у системі післядипломної педагогічної освіти : монографія. Запоріжжя : Кругозір, 2015. 532 с. URL: <https://surl.li/bkagtf> (дата звернення: 13.12.2024).
- Васильченко Л. В. Формування управлінської культури керівника школи в системі післядипломної педагогічної освіти : автореф. дис. ... канд. пед. наук : [спец.] 13.00.04 «Теорія і методика професійної освіти». Тернопіль, 2006. 23 с. URL: <http://dspace.tnpu.edu.ua/handle/123456789/1546> (дата звернення: 07.04.2024).
- Вініченко А. А. Особливості формування «культури управління» в сучасному соціумі. *Науковий вісник УМО «Педагогіка»*. 2016. № 1. URL: <https://surli.cc/eeeyzw> (дата звернення: 02.02.2025).
- Виноградський М. Д. Управління персоналом. URL: <http://pidruchniki.ws> (дата звернення: 12.12.2020).
- Гречаник О. Є., Грабар О. В. Професійне навчання як засіб розвитку корпоративної культури персоналу організації. *The Scientific Heritage*. 2021. No 81. VOL. 3. P. 29-32. URL: <https://surl.li/fxwnru> (дата звернення: 18.07.2024).
- Гречаник О. Є., Григораш В. В. Організація внутрішнього аудиту в закладі загальної середньої освіти: монографія. Харків : Основа, 2019. 144 с. URL: <https://surl.li/qqizvw> (дата звернення: 25.08.2024).
- Гречаник О. Є., Чупринін О. О. Управління розвитком творчої компетентності педагога. *Актуальні питання у сучасній науці. Сер.: Педагогіка*. 2023. № 1 (7). С. 362-374. DOI: [https://doi.org/10.52058/2786-6300-2023-1\(7\)](https://doi.org/10.52058/2786-6300-2023-1(7)).
- Григораш О. В. Акмеологічна оцінка управлінської культури керівника закладу освіти. *Освіта дорослих: світові тенденції, українські реалії та перспективи* : колект. моногр. Харків : ХНПУ, 2020. С. 255-260. URL: <https://surl.li/qiqnpi> (дата звернення: 10.10.2022).
- Гуцан Л. А. Компетентнісний підхід у сучасній освіті. *Формування базових компетентностей у вихованців позашкільних навчальних закладів*: Мат-ли Міжн. наук.-практ. конференції. Київ, 2013. С. 52-56. URL: <https://surl.li/nhmlta> (дата звернення: 14.05.2022).
- Єльнікова Г. В. Адаптивні технології в освіті Електронне наукове фахове видання «Адаптивне управління: теорія і практика». Серія «Педагогіка». 2017. № 3(5). URL: <https://surl.li/cjocdz> (дата звернення: 15.01.2025).
- Єльнікова Г. В. Компетентнісний підхід до моделювання професійної діяльності керівника вищого навчального закладу. *Теорія та методика управління освітою*. 2010. № 4. URL: <https://surl.li/kaujdg> (дата звернення: 11.09.2024).
- Закон України «Про повну загальну середню освіту». URL: <https://zakon.rada.gov.ua/laws/show/463-20#Text> (дата звернення: 02.12.2024).
- Закон України «Про освіту». URL: <https://zakon.rada.gov.ua/laws/show/2145-19#Text> (дата звертання: 02.12.2024).
- Інновації в управлінні закладами освіти: теорія та практика. Матеріали студентської науково-практичної конференції (10 листопада 2021 року). Харків : ХНПУ, 2021. 111 с. URL: <https://surl.li/necogs> (дата звернення: 17.06.2024).
- Ісаєва О. С., Єрченко О. В. Компетентнісний підхід як зміст освіти у медичних вишах. *Інноваційна педагогіка*. 2023. Т. 1. Вип. 64. С. 149-151. URL: <https://surl.li/czzqnd> (дата звернення: 12.11.2024).
- Касьянова О. М. Педагогічна експертиза як засіб сталого розвитку регіональної системи загальної середньої освіти. *Педагогіка формування творчої особистості у вищій і загальноосвітній школах*. 2013. Вип. 28. С. 381–387. URL: <https://surli.cc/inmbqt> (дата звернення: 22.02.2024).
- Касьянова О. М. Проектна діяльність як засіб розвитку управлінської культури викладача ВНЗ у системі післядипломного навчання. *Витоки педагогічної майстерності. Сер. : Педагогічні науки*. 2015. Вип. 15. С. 113-117. URL: <https://surl.li/ijwtxe> (дата звернення: 14.02.2025).
- Крамчанін В. М. Управлінська культура керівників закладів освіти як психолого-педагогічний

- феномен. URL: <https://surl.li/ytlwei> (дата звертання: 18.02.2023).
- Ксенофонтowa М. М., Заболотна Т. М. Управлінська культура: сутність та особливості формування. *Вісник Сумського національного аграрного ун-ту. Сер. : Економіка і менеджмент*. 2012. Вип. 8 (53). С. 81–86. URL: <https://surl.li/drxfko> (дата звернення: 26.12.2022).
- Леськова С. В. Компетентнісний підхід в управлінні кадровим потенціалом сучасного підприємства. *Трансформаційна економіка*. 2023. № 3. С. 26-31. DOI: <https://doi.org/10.32782/2786-8141/2023-3-5>.
- Луговий В. І. Компетентності та компетенції: поняттєво-термінологічний дискурс. *Вища освіта України. № 3 (додаток 1). Тематичний випуск «Педагогіка вищої школи: методологія, теорія, технології»*. Київ : Гнозис, 2009. С. 8-14. URL: <https://surl.li/chtvqp> (дата звернення: 15.09.2024).
- Мармаза О. І. Інноваційний менеджмент. Харків : ХНПУ, 2016. 197 с. URL: <https://surl.li/ensvte> (дата звернення: 22.10.2024).
- Мармаза О. І. Менеджмент освітньої організації. Харків : ТОВ «Щедра садиба», 2017. 126 с. URL: <https://surl.li/fjchcx> (дата звернення: 22.10.2024).
- Мармаза О. І. Стратегічний менеджмент. Харків : ТОВ «Планета-Прінт», 2015. 103 с. URL: <https://surl.li/woxcscz> (дата звернення: 22.10.2024).
- Мартинець Л. Функції управління професійним розвитком учителів. *Науковий вісник Ужгородського національного університету. Серія : Педагогіка. Соціальна робота*. 2016. Вип. 2. С. 137–139. URL: <https://surl.li/gsljow> (дата звернення: 17.11.2024).
- Нижник Н., Пашко Л. Управлінська культура: теоретичне поняття чи управлінська поведінка? *Політичний менеджмент*. 2005. № 5. С. 103-113. URL: <https://surl.li/kpoemm> (дата звернення: 12.04.2024).
- Новий освітній простір: Інформаційний посібник, 2019. URL: <http://www.minregion.gov> (дата звернення: 20.01.2020).
- Освітній менеджмент: навч. посіб. [за ред. Л. Даниленко, Л. Карамушки]. Київ : Шк. світ, 2003. 400 с. URL: <http://www.uaoppp.com.ua/read/70/> (дата звернення: 15.07.2024).
- Педагогічна творчість, майстерність, професіоналізм у системі підготовки освітянських кадрів: здобутки, пошуки, перспективи : монографія / керівн. авт. кол. Н. В. Гузій ; Мін-во освіти і науки України, Нац. пед. ун-т імені М. П. Драгоманова. Київ : Вид-во НПУ імені М. П. Драгоманова, 2015. 432 с. URL: <https://surl.li/stbkxc> (дата звернення: 14.03.2024).
- Перехейда О. Програма розвитку гімназії. Харків : Основа, 2012. 304 с. URL: <https://surl.li/cc/tlsget> (дата звернення: 15.10.2024).
- Пержун В. В. Методи дослідження управлінської культури в публічному управлінні. *Право та державне управління*. 2020. № 4. С. 146–152. URL: <https://surl.li/srejns> (дата звернення: 17.10.2024).
- Пержун В. В. Управлінська культура владних еліт сучасної України. *Вчені записки ТНУ імені В. І. Вернадського. Сер. : Державне управління*. 2020. Т. 31 (70). № 4. С. 16–21. URL: <https://surl.li/cc/zqfyjk> (дата звернення: 18.03.2024).
- Петрова І., Остапівський Б. Асоціативна модель компетенцій в управлінні ІТ проектом. *Вчені записки Університету «Крок»*. 2023. № 1 (69). С. 70-77. DOI: 10.31732/2663-2209-2022-69-70-77.
- Попова О. І. Компетентність та компетенція як наукові категорії: різноманітність підходів до вивчення сутності. *Теорія та практика державного управління*. 2012. Вип. 3. С. 193–200. URL: <https://surl.li/kdpxjt> (дата звернення: 15.10.2024).
- Поскрипко Ю. А., Данченко О. Б. Компетенція і компетентність: консенсус. *Вчені записки Університету «КРОК»*. 2019. № 3 (55). С. 117–127. DOI: <https://doi.org/10.31732/2663-2209-2019-55-117-127>.
- Пшенична Л. Управлінська культура менеджера освіти. *Педагогічні науки: теорія, історія, інноваційні технології*. 2020. № 8 (102). С. 368–382. URL: <https://surl.li/bfjfyj> (дата звернення: 08.03.2024).
- Рибалко Ю. В. Компетентнісний підхід у науково-педагогічній літературі. *Педагогіка вищої та середньої школи*. 2012. Вип. 35. С. 385-394. URL: <https://surl.li/kevcbj> (дата звернення: 16.11.2024).
- Розвиток системи управління закладом освіти : матеріали Всеукр. науково-практ. онлайн-конф. / [за

- заг. ред. проф. Р. Черновол-Ткаченко, проф. О. Мармази, доц. О. Гречаник]. Харків : ХНПУ імені Г. С. Сковороди, 2021. 326 с. URL: <https://surl.li/fkqzaz> (дата звернення: 14.10.2024).
- Ростовська В. І. Управлінська культура викладача вишу як важливий чинник результативності педагогічної діяльності. *Науковий огляд*. 2016. № 3 (24). С. 1–10. URL: <https://surl.li/rnluco> (дата звернення: 14.12.2023).
- Рудніцька К. В. Сутність понять «компетентнісний підхід», «компетентність», «компетенція», «професійна компетентність» у світлі сучасної освітньої парадигми. *Науковий вісник Ужгородського ун-ту. Сер. : «Педагогіка. Соціальна робота»*. 2016. Вип. № 1 (38). С. 241–244. URL: <https://surl.li/gmdnrl> (дата звернення: 15.03.2023).
- Савченко О. П. Компетентнісний підхід у сучасній вищій школі. *Педагогічна наука: історія, теорія, практика, тенденції розвитку*. 2010. № 3. URL: <https://surl.li/zfbplg> (дата звернення: 19.10.2023).
- Савчук Л., Бурлакова А. Розвиток корпоративної культури в Україні. *Персонал*. 2005. № 5. URL: <http://personal.in.ua/article.php?id=68> (дата звернення: 15.07.2023).
- Святоха В. А. Вплив управлінської культури керівника вищого навчального закладу на ефективність менеджменту. *Теоретичні і прикладні проблеми психології*. 2013. № 3 (32). С. 237–242. URL: <https://surl.li/ucylqq> (дата звернення: 14.07.2023).
- Синиченко А. В. Компетентнісний підхід як сучасна парадигма управління персоналом. *Фінанси, облік, банки*. 2016. № 1 (21). С. 288–294. URL: <https://surl.li/hntvrm> (дата звернення: 25.09.2024).
- Танько А. Теоретичні основи формування управлінської культури майбутніх менеджерів освіти. *Освітній простір України*. 2019. № 15. С. 130–136. DOI: <https://doi.org/10.15330/esu.15.130-136>.
- Тесленко Л. М. Управління якістю: практичні питання. *Управління закладами освіти в нових освітніх реаліях* / Мат-ли IV-ої студ. наук.-практ. конф. (10 лист. 2022 р. ; [за заг. ред. проф. Р. Черновол-Ткаченко, проф. О. Мармази, доц. О. Гречаник]. Харків : ХНПУ імені Г. С. Сковороди, 2022. 82 с. URL: <https://surl.li/copyxe> (дата звернення: 02.03.2024).
- Теоретичні і методичні засади моделювання фахової компетентності керівників закладів освіти: монографія / [Єльнікова Г. В., Зайченко О. І., Маслов В. І. та ін.] ; за ред. Г. В. Єльнікової. Київ-Чернівці : Книги – XXI, 2010. 460 с. URL: <https://surl.li/aebhvt> (дата звернення: 16.11.2024).
- Ткаченко В. П. Підготовка керівників закладів освіти у контексті європейської інтеграції. *Світоглядні пріоритети гуманізації вищої освіти: монографія* / за ред. В. І. Лугового, Ж. В. Таланової. Київ, 2017. С. 191–202. URL: <https://surl.li/qyhqej> (дата звернення: 09.08.2023).
- Смолич Д. В. Культура та етика керівника в управлінні організацією. *Економічні науки: зб. наук. пр. Луцького нац. техн. ун-ту. Сер. : Регіональна економіка*. 2021. № 18 (71). С. 180–191. DOI: [https://doi.org/10.36910/2707-6296-2021-18\(71\)-20](https://doi.org/10.36910/2707-6296-2021-18(71)-20).
- Шостак Л. В., Болодан Є. О. Зарубіжний досвід управління персоналом. *Приазовський економічний вісник*. 2018. Вип. 3 (08). URL: <http://inneco.org/article/view> (дата звернення: 17.04.2023).
- Ягунов В. В., Свистун В. І., Кришталь М. А., Король В. М. 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. URL: <https://surl.li/mwdgph> (дата звернення: 19.09.2023).
- Язловецька, О. В. Компетентнісний підхід як основа реформування освітнього процесу. *Наукові записки. Серія: Педагогічні науки*. 2022. № 206. С. 247–253. DOI: <https://doi.org/10.36550/2415-7988-2022-1-206-247-253>.
- Chomsky N. Aspects of the Theory of Syntax. Cambridge, MA : M.I.T. Press, 1965. 271 p. URL: <https://surl.li/ccgbvvwi> (дата звернення: 16.10.2022).
- Definition and Selection of Competencies. Country Contribution Process : Summary and Country Report. Uri Peter Trier. University of Neuchatel, October, 2001. 279 p. URL: <https://surl.li/cutffu> (дата звернення: 16.10.2022).
- McClelland D.C. Testing for Competence Rather Than for Intelligence. *American Psychologist*. 1973. № 28 (1). P. 1–14. URL: <https://surl.li/lspqg> (дата звернення: 18.10.2022).
- Spencer L., Spencer S. Competence at Work: Model for Superior Performance. New York : John Wiley & Sons, 1993. URL: <https://surl.li/ibjuxw> (дата звернення: 08.01.2023).

ДОДАТКИ

Додаток А

Анкета «Ваш творчий потенціал»

Мета: виявити творчий потенціал педагога.

Анкета складається з 18 закритих питань, кожне з яких має 3 варіанти відповідей.

Питання 1, 6, 7, 8 визначають межі зацікавленості, допитливості. Питання 2, 3, 4, 5 – віру в себе. Питання 9 та 15 – постійність. Питання 10 – амбіційність. Питання 11 – зорову пам'ять. Питання 12 і 13 – слухову пам'ять. Питання 14 – бажання бути незалежним. Питання 16 і 17 – здатність абстрагуватися. Питання 18 – ступінь зосередженості. Ці здатності і складають основні якості творчого потенціалу. Загальна сума набраних балів показує рівень педагогічної творчості.

Запитання:

1. Чи вважаєте ви, що оточуючий Вас світ може бути поліпшений: а) так; б) ні, він і так досить гарний; в) так, але тільки дечому.
2. Чи думаєте ви, що можете самі брати участь у значних змінах навколишнього світу: а) так, у більшості випадків; б) ні; в) так, у деяких випадках.
3. Чи вважаєте ви, що деякі з ваших ідей принесли б значний прогрес у тій сфері діяльності, у якій ви працюєте: а) так; б) так, за сприятливих обставин; в) лише в деякій мірі.
4. Чи вважаєте ви, що в майбутньому будете відігравати настільки важливу роль, що зможете щось принципово змінити; а) так, б) напевно; в) це мало ймовірно; в) можливо.
5. Коли ви вирішуєте почати якусь дію, чи думаєте ви, що здійсните своє починання: а) так; б) часто думаєте, що не зможете; в) так, часто.
6. Чи випробовуєте ви бажання зайнятися справою, що абсолютно не знаєте: а) так, невідоме вас приваблює; б) невідоме вас не цікавить; в) все залежить від характеру цієї справи.
7. Вам доводиться займатися незнайомою справою. Чи випробуєте ви бажання домогтися в ньому досконалості: а) так; б) задовольнитесь тим, чого встигли домогтися; в) так, але тільки якщо це вам подобається.
8. Якщо справа, яку ви не знаєте, вам подобається, чи хочете ви знати про неї все: а) так; б) ні, ви хочете навчитися тільки найголовнішому; в) ні, ви хочете тільки задовольнити свою цікавість.
9. Коли ви зазнаєте невдачі, ви: а) якийсь час продовжуєте справу всупереч здоровому глузду; б) махнете рукою на цю витівку, тому що розумієте, що вона нереальна; в) продовжуєте робити свою справу, навіть коли очевидно, що перешкоди непереборні.
10. На вашу думку, професію треба вибирати, виходячи з: а) своїх можливостей, подальших перспектив для себе; б) стабільності, значимості, потреби професії, потреб у ній; в) переваг, які вона забезпечить.
11. Подорожуючи, могли б ви легко орієнтуватися у маршруті, по якому вже пройшли: а) так; б) ні, боїтеся збитися зі шляху; в) так, але тільки там, де місцевість вам сподобалася.
12. Відразу ж після якоїсь бесіди чи зможете згадати все, що говорилося; а) так, без зусиль; б) усього згадати не можете; в) запам'ятовуєте тільки те, що вас цікавить.

13. Коли ви чуєте слово незнайомою для вас мовою, то можете повторити його по складах, без помилки, навіть не знаючи його значення: а) так, без утруднень; б) так, якщо це слово легко запам'ятати; в) повторите, але не зовсім правильно.
14. У вільний час ви віддаєте перевагу: а) залишатися наодинці, помізкувати; б) перебувати в компанії; в) вам байдуже, чи будете ви одні або в компанії.
15. Ви займаєтеся якоюсь справою. Вирішуєте припинити це заняття тільки тоді, коли: а) справа закінчена й здається нам відмінно виконаною; б) ви більш-менш задоволені; в) вам ще не все вдалося зробити.
16. Коли ви од(на)ин; а) любите мріяти про якісь навіть, може бути, абстрактні речі; б) будь-якою ціною намагаєтеся знайти собі конкретне заняття; в) іноді любите помріяти, але про речі, які пов'язані з вашою роботою.
17. Коли якась ідея захоплює вас, то ви станете думати про неї:
а) незалежно від того, де й з ким ви перебуваєте; б) ви можете робити це тільки наодинці; в) тільки там, де буде не занадто галасливо.
18. Коли ви відстоюєте яку-небудь ідею: а) можете відмовитися від неї, якщо вислухаєте переконливі аргументи опонентів; б) залишитеся при своїй думці, які б аргументи не вислухали; в) змініте свою думку, якщо опір виявиться занадто сильним.

Додаток Б

Кваліметрична модель оцінки якості управління розвитком творчої компетентності педагогів

Фактори	Вагомість	Критерії	Вагомість	Показники	Коеф. відпов.
1. Інформаційне забезпечення управління розвитком творчої компетентності $\Phi 1 = m1 (V1K1 + V2K2 + V3K3)$	$m1=0,12$	1. Наявність і усвідомлення мети роботи та образу кінцевого результату. 2. Наявність і рівень систематизації існуючої інформації. 3. Своєчасність доведення зовнішньої та внутрішньої інформації до учасників освітнього процесу	$V1=0,3$ $V2=0,2$ $V3=0,5$	1. Обізнаність членів колективу з кінцевим результатом, наявність моделі творчого педагога і випускника ЗЗСО. 2. Інформаційний банк даних, протоколи нарад, педрад тощо. 3. Обізнаність адміністрації та педагогів з інформацією щодо стану роботи над проблемою.	
2. Науковість роботи з розвитку	$m2=0,15$	4. Дотримання принципів	$V4=0,25$	4. Конкретність, перспективність, об'єктивність	

творчої компетентності Ф2 = m2 (V4K4+V5K5+V6K6)		управлінської діяльності.		запланованих заходів для підвищення рівня творчої компетентності педагогів.	
		5. Підготовка науково обґрунтованих рекомендацій щодо засобів ліквідації помічених недоліків.	V5=0,5	5. Накази, аналітичні довідки, звіти про проміжні результати роботи над проблемою.	
		6. Використання досягнень сучасної науки.	V6=0,25	6. Володіння сучасними технологіями, методами, прийомами, формами для управління роботою з розвитку творчої компетентності	
3. Розподіл управлінської праці між членами адміністрації з питань розвитку творчої компетентності Ф3 = m3 (V7K7+V8K8+V9K9+V10K10)	m3=0,14	7.Охоплення всіх напрямів управлінської діяльності.	V7=0,4	7.Модель організаційної діяльності закладу.	
		8.Відсутність дублювання в розподілі обов'язків.	V8=0,1	8. Організація роботи з розвитку творчої компетентності з усіма учасниками освітнього процесу.	
	m4=0,15	9.Оптимальність навантаження.	V9=0,2	9.Функціональні обов'язки керівної ланки.	
4. Організація особистої праці керівників з проблеми дослідження Ф4 = m4 (V11K11+V12K12+V13K13+V14K14)		10.Відповідність діяльності функціональним обов'язкам.	V10=0,3	10.Обсяг та напрямки роботи.	
		11.Наявність циклограм управлінської діяльності.	V11=0,6	11. Наявність методичного дня.	
		12. Наявність алгоритмів діяльності.	V12=0,05	12. Матеріали роботи: звіти, довідки, накази.	
			V13=0,2	13. Річний план роботи школи.	
			V14=0,15	14.План роботи на тиждень.	

		<p>13. Наявність планів роботи на тиждень.</p> <p>14. Наявність особистих планів роботи керівників на день.</p>		15. Планування роботи завідуючої, педагога-методиста, психолога	
<p>5. Забезпечення раціональної праці підлеглих з розвитку творчої компетентності педагогів Ф5 = m5 (V15K15+ V16K16+V17K17)</p>	m5=0,13	<p>15. Планування робочого часу педагогів.</p> <p>16. Оптимальність режиму навчального закладу.</p> <p>17. Підбір виконавців відповідно до їх функціональних обов'язків та особистих можливостей</p>	<p>V15=0,3</p> <p>V16=0,2</p> <p>V17=0,5</p>	<p>16. Розклад занять у групах, розклад роботи гуртків, секцій, студій.</p> <p>17. Дотримання нормативних документів, санітарно-гігієнічних вимог.</p> <p>18. Матеріали нарад, протоколи методичної ради, МО</p>	
<p>6. Створення умов для розвитку педагогічної творчості, творчої компетентності Ф6 = m6 (V18K18+ V19K19+V20K20+ V21K21+ V21K21)</p>	m6=0,14	<p>18. Забезпеченість науково-методичною літературою з розвитку творчої компетентності.</p> <p>19. Забезпеченість технічними засобами навчання та виховання.</p> <p>20. Психологічна підтримка.</p> <p>21. Наявність системи морального та матеріального стимулювання.</p>	<p>V18=0,15</p> <p>V19=0,15</p> <p>V20=0,3</p> <p>V21=0,2</p>	<p>19. Періодичні видання.</p> <p>20. Нові методичні надходження.</p> <p>21. Забезпеченість необхідними навчальними матеріалами.</p> <p>22. Обладнання кабінетів.</p> <p>23. Обладнання студій.</p> <p>24. Використання ІКТ для оброблення інформації.</p> <p>25. Психодіагностична робота.</p> <p>26. Корекційна робота.</p> <p>27. Шкала моральних і матеріальних заохочень.</p> <p>28. Накази про заохочення, преміювання, надання додаткових відпусток тощо.</p>	

		22. Створення позитивного психологічного клімату	V22=0,2	29. Результати психологічного дослідження.	
7. Результативність роботи з розвитку творчої компетентності Ф7 = m7 (V23K23+ V24K24+ V25K25+ V26K26+ V27K27+ V28K28+ V29K29)	m7=0,17	23. Підвищення кваліфікаційного рівня педагогів.	V23=0,2	30. Атестаційні матеріали. 31. Створення творчих груп педагогів. 32. Проведення відкритих занять та виховних заходів.	
		24. Наявність науково-експериментальних досліджень.	V24=0,09	33. Проведення науково-практичних семінарів, конференцій, управлінських майстерень.	
		25. Творчий характер виступів на педагогах.	V25=0,075	34. Протоколи засідань, матеріали виступів.	
		26. Публікації педагогів.	V26=0,075	35. Друковані праці, видання книжок, розробки занять, виховних заходів.	
		27. Узагальнення передового педагогічного досвіду.	V27=0,06	36. Картотека ППД з розвитку педагогічної творчості.	
		28. Рівень досягнень здобувачів освіти.	V28=0,2	38. Творчі досягнення: співи, музика, танці, живопис, література, прикладне мистецтво, інтелект. конкурси.	
		29. Загальний рейтинг ЗДО.	V29=0,3	39. Спортивні досягнення. 40. Ставлення до школи здобувачів, батьків, громадськості. 41. Рейтинг ЗЗСО серед інших ЗО	

CHAPTER 7. DIGITAL ECONOMY AND INFORMATION SECURITY IN INTERNATIONAL SECURITY SYSTEMS

Serhii DEMENTIEV

candidate of Technical Sciences (Ph. D.)

Associate Professor at Vinnytsia Trade and Economic Institute, Department of
Information Systems and Technologies,
(25, Khmelnytske shose, Vinnytsia, 21050, Ukraine)

s.dementiev@vtei.edu.ua

<https://orcid.org/0009-0006-1322-6756>

Svitlana MERINOVA

candidate of Economic Sciences (Ph. D.)

Associate Professor at Vinnytsia Trade and Economic Institute, Department of
Information Systems and Technologies,
(25, Khmelnytske shose, Vinnytsia, 21050, Ukraine)

s.merinova@vtei.edu.ua

<https://orcid.org/0000-0001-6563-5320>

Abstract. The monograph is dedicated to exploring the role of the digital economy and information security within the context of international security systems. The authors analyze contemporary challenges related to cyber threats, financial fraud, and economic espionage that arise from the rapid digitalization of economic processes. The work examines innovative approaches to countering economic threats in cyberspace, including the use of artificial intelligence, blockchain, quantum cryptography, and the Zero Trust concept. Special attention is given to risk management in the digital economy, international experience in regulating digital finance, and the implementation of central bank digital currencies (CBDCs). The research results emphasize the need for a comprehensive approach to ensuring economic security, including the development of cyber diplomacy, harmonization of international cybersecurity standards, and enhancing digital literacy among the population. The monograph offers recommendations for minimizing risks and creating a stable digital environment for the further development of the global economy.

Keywords: digital economy, information security, cybersecurity, risk management, cyber diplomacy, economic espionage, zero trust concept.

Introduction. In the modern world, digital transformation plays a key role in the development of the economy, public administration, and business security. Information technologies have become not only a tool for increasing productivity but also an important factor in ensuring the economic security of nations. The digitalization of economic processes enhances the efficiency of financial management, international trade, and the optimization of production chains. However, the digital economy also creates new challenges related to cyber threats, financial fraud, economic espionage, and the vulnerability of state information systems.

In the face of global threats, it is crucial to develop effective risk management strategies and ensure the cyber resilience of economic processes. The implementation of

innovative information technologies, such as artificial intelligence, blockchain, big data, quantum cryptography, and automated risk monitoring systems, is of particular importance. Global economic stability depends on the effectiveness of digital defense mechanisms, including forecasting systems, financial monitoring, and cyber diplomacy.

The relevance of this research is driven by the rapid growth of cyber threats affecting the financial sector, public administration, and international relations. The high dependence on digital technologies makes the global economy more vulnerable to attacks, manipulation of economic data, and crisis phenomena, necessitating a comprehensive approach to the protection and regulation of the digital economy.

The aim of this research is to analyze the role of information technologies in ensuring economic security, assess the main risks arising in the digital economy, and develop recommendations for their mitigation. The study also covers an analysis of international experience in regulating digital finance, combating cybercrime, and the use of digital currencies in the global economy.

To achieve this goal, the following research methods were used:

Analysis and synthesis — assess current trends in cybersecurity;

Comparative analysis — study international experience in managing digital risks;

Forecasting — evaluate potential threats and develop strategies to prevent them;

Statistical analysis — assess the economic impact of cyber threats on global financial systems;

Modeling — digital tools analyze the effectiveness in ensuring financial security.

The research is based on official reports from international financial organizations, statistical data from central banks, publications in scientific journals, analytical reports from government and private analytical centers, as well as information from open sources (OECD, IMF, World Economic Forum, World Bank).

- The object of the research — digital technologies and their impact on the economic security of states and businesses.

- The subject of the research — mechanisms, methods, and tools for ensuring security in the digital economy, as well as information systems used for risk management and the protection of critical infrastructure.

This research is relevant in the context of global changes and the digitalization of the world economy, as it allows not only to identify the main risks but also to propose effective mechanisms for managing information security in the economic branches.

The digital economy as a strategic factor in international security. The digital economy is a key factor in global development, influencing world economic processes, international security, and the competitiveness of nations. It promotes productivity growth, enhances business efficiency and public administration, creating new opportunities for international cooperation.

A new digital economy is also brings new challenges: cyber threats, unequal access to digital technologies, digital assets regulating issues, and data privacy. On one hand, digitalization opens access to new financial instruments, reduces business costs, and enhances the efficiency of public administration (*The Global Risks Report, 2021*). On the other hand, it increases dependence on digital infrastructure, creating new risks, such as:

- Increased cyberattacks on government institutions and private companies,

- The danger of digital inequality due to unequal access to technologies,
- Job losses in traditional sectors due to automation.

Modern enterprises are adapting to the digital economy through:

- Automation of business processes and the use of AI for data analysis.
- Integration of blockchain solutions to enhance transaction security.
- Use of Big Data to improve marketing strategies and risk management.

Table 1.1 – Digital economy development over the last 5 years chronology

<i>Year</i>	<i>Event</i>
2019	Increased popularity of blockchain solutions for financial transactions.
2020	The development of remote work due to the COVID-19 pandemic contributed to the rapid growth of digital services.
2021	Active use of artificial intelligence in financial and banking systems.
2022	Countries began testing central bank digital currencies (CBDCs).
2023	Implementation of AI regulation in the EU, development of the digital yuan in China.
2024	Investments in financial technologies increased by 30%, and the blockchain solutions market grew by 200%.

Table 1.2 – Digital economy growth dynamics

<i>Indicator</i>	<i>2019</i>	<i>2020</i>	<i>2021</i>	<i>2022</i>	<i>2023</i>	<i>2024</i>
The digital economy in global GDP share (%)	15	17	19	21	23	25
The digital economy in Ukraine's GDP share (%)	6	7	8	9	10	12
Investments in fintech (billion USD)	150	180	210	250	280	320

The modern economic system faces numerous threats, particularly in the areas of financial security, the digital economy, and international financial relations. The main threats include:

- Cyberattacks on financial institutions — for example, the 2016 attack on the SWIFT system, which resulted in losses of hundreds of millions of dollars. Hackers exploited vulnerabilities in banking systems to conduct unauthorized transactions.
- Use of artificial intelligence by cybercriminals — AI can create sophisticated malware that bypasses traditional security systems. Deepfake technologies are also used for fraud in the financial sector.
- Risk of data breaches — weak systems for protecting personal and financial information can lead to large-scale abuses, including financial fraud and blackmail.
- Rising economic inequality — the digital transformation of the economy creates new challenges for the labor market, as automation displaces part of the workforce, exacerbating social tensions.
- Risks associated with the implementation of digital currencies (CBDCs) — they could alter financial flows and global balances, leading to new forms of economic confrontation between countries (*Гуз А. М., Ткачук Т. Ю., 2020*).

The following graph illustrates the growth in the efficiency of digital technology usage in recent years.

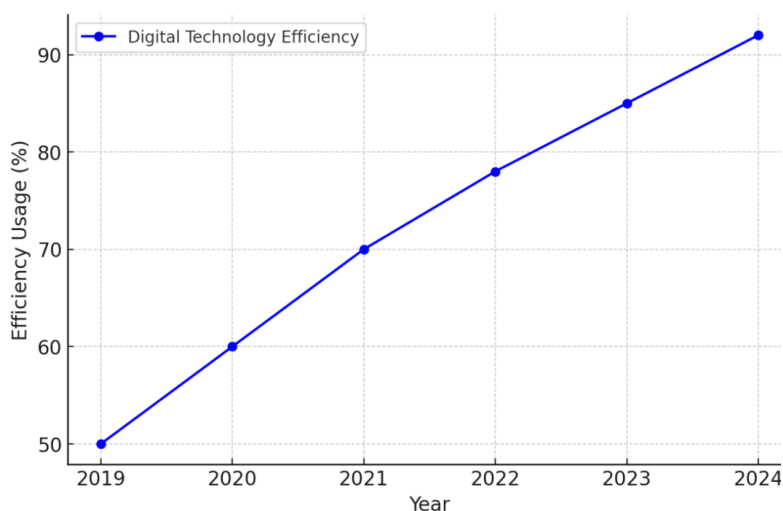


Figure 1.1 – Increasing efficiency in the use of digital technologies

To mitigate risks in the financial and economic sectors, the following approaches are applied:

- Use of blockchain technologies — this ensures transparency and security of financial transactions. Decentralized ledgers reduce the likelihood of fraud and manipulation.
- Regular updates of security systems — banks and financial institutions must continuously improve their cybersecurity mechanisms, implementing multi-factor authentication and threat detection systems.
- Development of artificial intelligence for threat monitoring — automated algorithms analyze anomalies in financial flows in real-time, enabling quick responses to potential cyberattacks.
- Development of regulatory frameworks — governments and financial regulators are developing laws to protect digital financial assets and combat fraud (*Soomro, 2015*).
- Enhancing financial literacy — citizens and businesses must be aware of financial risks and methods of protecting personal data.

China is actively promoting the digital yuan (e-CNY) as a tool for international settlements. Pilot programs are operating in over 20 cities, including Shanghai and Beijing. The use of the digital yuan in international trade could reduce China's dependence on the US dollar and strengthen its economic influence.

The European Central Bank (ECB) is exploring the possibility of launching a digital euro. The main goal is to reduce risks associated with private cryptocurrencies and ensure the stability of the financial system.

The Federal Reserve System (Fed) is testing the concept of a digital dollar. The US views CBDCs as a tool to increase payment efficiency and competitiveness in the global financial market (*Dwivedi et al., 2020*).

Impact of CBDC Implementation on the Global Economy.

The implementation of state digital currencies could significantly change the balance in the global financial system and lead to the following consequences:

- Reduced role of the US dollar in international transactions — China and other countries may switch to alternative digital currencies, weakening the dominance of the dollar (*The Global Risks Report, 2021*).

- Increased control over financial flows in authoritarian countries — governments will be able to more accurately track transactions and control economic activity.

New forms of economic confrontation — competitive struggles for leadership in digital financial technologies between the US, China, and the EU could lead to increased economic sanctions and regulatory restrictions.

Increased efficiency of international payments — digital currencies could significantly reduce the costs of international transfers and speed up their processing.

The digital economy fundamentally changes social and economic processes worldwide, creating new opportunities and challenges. The implementation of digital technologies affects employment, income inequality, access to education and public services, as well as the transformation of business and public administration.

How the Digital Economy Affects Society and the Economy.

First, automation and transformation of the labor market. About 40% of traditional professions may disappear by 2040 due to automation and the use of artificial intelligence. In 2023, over 85% of large companies invested in the automation of business processes, which allows reducing costs and increasing labor productivity. Demand for new professions in cybersecurity, data analysis, and artificial intelligence is growing by an average of 20% annually.

Second, the expansion of digital inequality. A high level of digital literacy provides advantages in the labor market, while populations with low technical skills face the risk of marginalization. In 2023, over 3.5 billion people worldwide still did not have access to high-speed internet, limiting their economic opportunities. Innovative states such as Singapore, Estonia, and Finland are actively investing in digital education and technological infrastructure, reducing the gap between different social groups.

Third, the transformation of business and financial systems. The use of digital platforms, marketplaces, and e-commerce has significantly increased business productivity: online trade volumes grew by 27% in 2023. Financial technologies (FinTech) allow small businesses to access global markets, reducing dependence on traditional banking services. Innovative financial instruments, such as CBDCs (central bank digital currencies), are changing the monetary policies of states.

Fourth, the impact of digitalization on public administration. The introduction of e-government contributes to increased transparency and reduced levels of corruption. In Ukraine, the "Diia" system has automated over 70 public services and reduced the administrative burden on businesses. Digital identification and Big Data analytics improve the efficiency of social programs and the tax system.

These initiatives demonstrate that governments are actively implementing strategies to support digital literacy, as it is a key condition for economic growth and innovative development.

The digital economy creates vast opportunities, but its development requires a balanced approach to risk management, enhancing digital literacy, and adapting to global changes. A systematic approach to supporting digital competencies among the population and businesses is the key to stable economic growth and security in the future.

Ensuring digital literacy among the population is a key factor for economic competitiveness and reducing social inequality. Various countries are implementing government programs to prepare citizens for the digital economy (Table 1.3).

Table 1.3 – Government programs for preparing citizens for the digital economy

<i>Country</i>	<i>Program</i>	<i>Main measures</i>	<i>Expected results</i>
EU	Digital Skills & Jobs Coalition	Training 20 million Europeans for work in the digital economy	Reducing digital inequality
US	National AI Initiative	Investments in education in programming, cybersecurity, and AI	Increasing the number of AI specialists by 30% by 2027
Ukraine	Diia.Osvita	Online courses on digital literacy, educational initiatives for pensioners	Increasing the level of digital literacy among the population
Estonia	e-Estonia	Full digitalization of education, public services, and the banking sector	99% of public services available online
Singapore	SkillsFuture	Grants for retraining citizens for work in the technology sector	Creating new jobs in the digital technology sector

The digital economy plays a strategic role in international security and the development of the global financial system. Innovative technologies make financial operations more efficient but also create new threats. The implementation of CBDCs could fundamentally change the balance of power in the global economy, leading to new challenges in international financial security. The economic system of the future must adapt to digital transformation, ensuring security, stability, and inclusivity in various areas.

The digital economy as a strategic factor in international security. Economic security is a critical factor for the stable functioning of businesses and the state. Information systems play a key role in ensuring financial monitoring, protecting businesses from threats, and supporting critical infrastructure. They contribute to improving the performance of enterprises by automating processes, enhancing control over financial flows, and ensuring effective risk management.

The following key factors influence economic security:

- Cyber threats — increased attacks on financial institutions, data breaches, and hacker attacks on critical infrastructure.
- Financial stability — the ability to effectively manage financial flows and forecast risks.
- Automation — the level of integration of digital solutions into business processes of enterprises and government institutions.
- Globalization — the impact of international markets and financial crises on the economic stability of a country.

- Digital transformation — the use of advanced information technologies to improve the efficiency and security of economic processes.

Factor analysis allows assessing how different factors affect the economic security of an enterprise. The main groups of factors are:

- Technological — the speed of implementation of information systems determines the competitiveness of a company.

- Financial — the presence of a stable financial model contributes to effective protection against risks.

- Regulatory — changes in legislation may require additional security measures and the implementation of new data protection systems.

- Personnel — the level of employee qualifications in information security affects the level of threats.

Information systems allow companies to:

- Optimize operational processes and reduce costs.
- Improve management decision-making through data analytics.
- Enhance protection against financial and cyber threats.
- Automate control of financial flows to prevent fraud.
- Use artificial intelligence and big data to forecast market trends.

The automation of economic processes is a key factor in ensuring financial stability and the security of enterprises. Information systems such as ERP and CRM enable enterprises to effectively manage resources, minimize risks, and ensure the continuity of business processes.

Below is a list of 20 information systems that impact economic security.

Table 1.4 – Main Information Systems

<i>Nº</i>	<i>Information System</i>	<i>Purpose</i>	<i>Examples</i>
1	Financial monitoring automation	Detection of suspicious financial transactions and prevention of money laundering	Actimize, SAS AML
2	ERP systems (Enterprise Resource Planning)	Optimization of company resource management, reduction of fraud risks	SAP ERP, Oracle ERP Cloud
3	CRM systems (Customer Relationship Management)	Protection of customer data and management of interaction with customers	Salesforce, Microsoft Dynamics 365
4	Risk Management Systems (RMS)	Prediction of financial threats	MetricStream, RiskWatch
5	Blockchain technologies	Ensuring transparency of transactions and protection against fraud	Hyperledger, Ethereum, IBM Blockchain
6	Biometric authentication systems	Fingerprint verification, facial recognition	BioID, FaceTec
7	Cybersecurity information systems	Protection against cyberattacks on financial institutions and enterprises	IBM Security QRadar, Palo Alto Networks
8	Intelligent analytical systems	Detection of financial fraud using AI	Splunk, Darktrace
9	Financial flow monitoring systems	Control of cash flows by central banks	SWIFT, FinCEN
10	Access control systems	Protection of financial institutions from unauthorized access	Okta, Microsoft Azure AD

11	Cybersecurity for critical infrastructure	Protection of energy, transport and financial networks	Cisco SecureX, Fortinet
12	Cloud data management platforms	Protection of information from leaks and unauthorized access	Google Cloud Security, AWS Shield
13	Big data analysis systems	Prediction of economic threats	Hadoop, Apache Spark
14	Automated financial management systems	Optimization of enterprise expenses and control of budgets	SAP S/4HANA Finance, Oracle Financials Cloud
15	Fraud prevention systems	Detection and blocking of suspicious financial transactions	IBM Trusteer, Feedzai
16	Economic risk forecasting systems	Analysis of macroeconomic trends	Moody's Analytics, FICO Score
17	Automated stock trading systems	Management of investments in financial markets	MetaTrader, Bloomberg Terminal
18	Crisis management systems	Responding to economic and financial crises	Everbridge, D4H
19	Payment information systems	Ensuring the security of transactions and international payments	Visa Secure, PayPal Fraud Protection
20	Darknet monitoring systems	Detection of threats, related to financial fraud	Recorded Future, DarkOwl

In Ukraine, the digitalization of the economy is accelerating, contributing to the increased efficiency of government and commercial institutions. However, there are several challenges that affect the overall level of security:

Development of cyber threats — the number of attacks on government websites, financial institutions, and critical infrastructure is increasing.

Innovative financial solutions — the digital hryvnia and the active development of cashless payments contribute to faster integration into international financial systems (Войціховський А. В., 2020).

European integration — adaptation to European digital security standards requires significant resources and reforms in the field of information policy.

Globally, there is active development of digital technologies that impact financial systems and cybersecurity:

- The European Union and the US — are actively developing central bank digital currencies and strengthening control over digital finance and cybersecurity.
- China — is actively using the digital yuan for international settlements, which is changing the balance of the global financial system.
- Technology corporations — global companies such as Google, Microsoft, and Amazon are implementing new data protection standards and using artificial intelligence for cybersecurity.
- Digital technologies are shaping a new model of economic security, ensuring data and infrastructure protection:
 - Artificial intelligence — provides automated detection of threats in financial operations and analysis of anomalies.
 - Blockchain — creates transparent mechanisms for managing financial transactions and minimizes the risks of fraud.

- Cloud technologies — ensure data storage and security, allowing companies to work in any environment.

- Internet of Things — is used to monitor the status of industrial facilities, transportation, and critical infrastructure.

Information systems are a defining factor in economic security, contributing to the automation of business processes and improving the performance of enterprises. Ukraine is actively developing its digital economy but faces challenges in the field of cybersecurity. On an international scale, digital technologies are changing the balance of power, requiring new security strategies.

Innovative approaches to countering economic threats in cyberspace. In the modern world, economic threats arise not only from traditional challenges such as inflation, resource shortages, or economic crises but also from rapid changes in the digital sphere. New challenges require new solutions, and innovation is key to increasing the resilience of economic systems and their adaptability to change. The application of advanced technologies such as artificial intelligence, cryptography, and the Zero Trust concept enables not only the prevention of threats but also their prediction and effective response.

Why is it important to apply innovation in the field of economic security?

Dynamics of threat development — Cybercriminals, fraudsters, and unscrupulous competitors are constantly improving their methods, creating new attack schemes targeting financial systems, logistics, production, and even national security. The use of traditional defense methods is no longer sufficient, as threats become more complex and unpredictable.

Adaptation to the digital economy — The world is transitioning to digital business models, and enterprises that do not adopt modern technologies risk losing their competitive advantages. For example, artificial intelligence helps optimize production processes, analyze market trends, and minimize risks.

Countering global challenges — Economic security is no longer confined to the borders of one country. Global crises, trade wars, financial manipulations, and sanctions policies are changing the economic balance of power in the world. The use of advanced technologies allows countries and businesses to protect themselves from financial and trade attacks.

Effective forecasting and analytics — Innovative technologies enable not only the detection of problems but also their prediction. Artificial intelligence algorithms can analyze large volumes of data and predict crisis situations, preventing economic losses (*Кольцова І., 2018*).

Increasing trust in economic systems — Investors, partners, and consumers seek to collaborate with companies and states that ensure a high level of economic security. The use of Zero Trust technologies, cryptographic data protection methods, and blockchain solutions strengthens trust in financial operations and commercial activities.

The EU is actively implementing regulatory mechanisms to enhance economic security through the use of digital technologies. In particular, cybersecurity directives (NIS2) require enterprises to implement multi-level protection systems, including blockchain solutions to prevent economic crimes.

In the US, innovations in economic security are focused on the public sector and strategic industries. Financial institutions use AI systems to detect fraud, and the Zero Trust concept has become a standard in many government agencies.

China is investing in the development of quantum cryptography and blockchain technologies, ensuring the security of the digital yuan and international financial operations.

Ukraine is gradually integrating innovations into the field of economic security, particularly in the protection of state registries, digital identification, and automated financial monitoring. In the context of war and economic instability, digital technologies play an important role in stabilizing the financial system.

Artificial intelligence (AI) and machine learning are powerful tools for detecting and predicting economic crises, analyzing large volumes of data, and identifying anomalies in financial transactions. They help governments and businesses respond to potential risks at an early stage.

Main Directions of AI Application in Economic Security:

- Monitoring financial transactions — detecting anomalous transactions and financial fraud.
- Forecasting economic crises — analyzing macroeconomic indicators and warning of potential crisis situations.
- Risk management — assessing credit risks and preventing economic sabotage.
- Labor market analysis — forecasting changes in employment, assessing labor productivity.

According to the IMF, 75% of financial institutions worldwide use AI to assess risks and prevent fraud. In 2023, the global AI market in economic analysis exceeded 20 billion USD, and by 2028 it is expected to grow up to 50 billion.

The security of the economic system depends on the level of data protection. The use of cryptographic algorithms and the Zero Trust concept significantly reduces the risk of cyberattacks and financial fraud.

Table 1.5 – Use of AI for Risk Assessment and Fraud Prevention

<i>Country</i>	<i>Use of AI in the Financial Sector (%)</i>	<i>Expected Market Growth by 2028 (billion USD)</i>
US	85%	22
EU	78%	18
China	90%	25
Ukraine	50%	5

Main Methods of Cryptographic Protection:

- Blockchain — the technology ensures the transparency of financial transactions and prevents document forgery.
- Data encryption — protection of information in banking operations, state registries, and corporate systems.
- Electronic signatures — confirmation of the authenticity of digital documents.
- Zero Trust technology — verification of all users and devices interacting with systems.

The global blockchain technology market in financial security was valued at 12.4 billion USD in 2023. It is expected to reach 60 billion by 2030. The US and China are investing over \$10 billion annually in the development of Zero Trust.

Financial and economic security is increasingly becoming a target of information warfare. The use of cybercrime schemes to manipulate economic processes creates new threats for states and businesses.

Main Methods of Financial Terrorism and Cyber Threats:

- Market manipulation — destabilization of currency exchange rates, falsification of economic data.
- Hacker attacks on the banking system — interference in financial transactions, blocking of payments.
- Economic blackmail — sanctions, restrictions on access to financial resources, control over international payment systems.
- Disinformation — fake news about the economic situation, affecting investors.

In 2022, global financial losses from cybercrime exceeded \$10.5 trillion USD, almost equal to China's GDP. According to the European Cybersecurity Agency, attacks on the banking sector increased by 300% over the past three years.

Table 1.6 – Losses from Cybercrime (billion USD)

<i>Country</i>	<i>Losses from Cybercrime (billion USD)</i>	<i>Increase in Bank Attacks (%)</i>
US	3,2 trillion	250%
EU	1,8 trillion	220%
China	2,5 trillion	310%
Ukraine	20 billion	400%

Innovative approaches to countering economic threats in cyberspace are key to ensuring the stability of national economies and the international financial system (Біленчук П.Д., 2018). The use of modern technologies such as artificial intelligence, cryptography, Zero Trust, and analytical threat modeling enables effective risk prevention.

The development of quantum computing and quantum cryptography could change approaches to ensuring financial security, risk management, and the protection of critical digital infrastructures. The development of quantum cryptography for the protection of financial operations. Quantum algorithms, such as the BB84 protocol, ensure absolute security of transmitted information, as any attempt to intercept it alters its content.

Major financial institutions such as JPMorgan Chase and Bank of America are already testing quantum cryptographic solutions to protect international transactions. The threats posed by quantum computers to existing security systems. RSA and ECC algorithms, which are used to encrypt most financial data, can be broken by quantum computers, posing a threat to traditional cryptographic systems. Google announced in 2019 the achievement of "quantum supremacy," signaling to governments and companies the need to transition to post-quantum cryptography. Examples of international organizations in the field of quantum communications: the OpenQKD project, funded by the EU, tests quantum cryptography for the protection of digital communications. IBM and Microsoft are developing quantum cloud computing, which could change approaches to processing large financial data. The quantum satellite network Micius provides a secure communication channel between key financial centers.

Artificial intelligence (AI) is becoming a key tool in the field of financial security, risk forecasting, and transaction management. AI analyzes macroeconomic indicators, market behavior, and payment statistics, enabling the prediction of financial crises. For

example, BlackRock Aladdin's analytical systems in 2022 were able to predict changes in global investment flows based on big data.

AML (Anti-Money Laundering) systems based on AI automatically track suspicious transactions using deep learning methods. PayPal and Visa have implemented AI systems to detect fraudulent operations, reducing financial losses by 40% (*The Global Risks Report, 2021*).

The growth of Web 3.0 and metaverses is impacting financial markets, business models, and the regulation of digital assets. The use of smart contracts based on Ethereum and Polkadot reduces the need for intermediaries in financial transactions. DAOs (decentralized autonomous organizations) create new forms of digital business management without centralized control.

The development of NFTs and smart contracts in international trade. NFTs (non-fungible tokens) are used to verify ownership of digital assets, promoting the development of new markets in art, real estate, and collectibles. Major companies such as Adidas and Gucci have already integrated NFTs into their business models to expand customer interactions.

For practical application, a model for countering economic threats in cyberspace can be proposed. It should include a comprehensive approach that combines technological, organizational, and international aspects of security.

The model consists of four key levels (Figure 1.2):

- 1. Threat forecasting
- 2. Prevention and preventive measures
- 3. Operational response
- 4. Analysis and adaptation of strategies

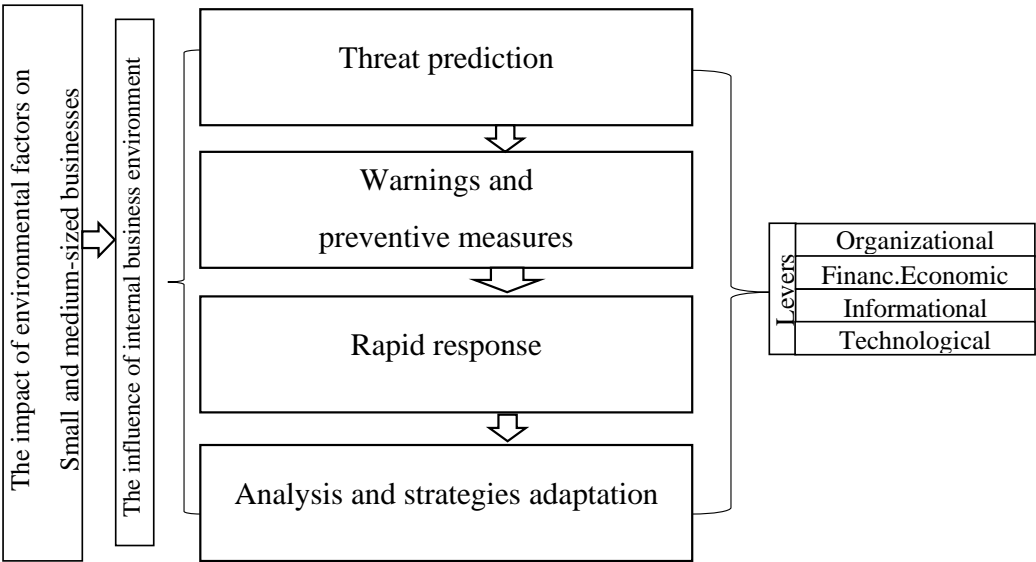


Figure 1.2 - Model for countering economic threats in cyberspace

Regulatory aspects of cryptocurrencies and asset tokenization. The MiCA (Markets in Crypto-Assets) regulation establishes requirements for the registration of cryptocurrency exchanges and the protection of investor rights. The SEC has intensified oversight of

cryptocurrency projects, defining legal frameworks for the regulation of tokenized assets (US). One of the first markets to introduce a legal framework for STO (Security Token Offering), allowing the use of tokenized assets in corporate finance (Japan).

The digital economy is in a stage of global transformation, and the further development of these technologies will be a key factor in shaping the financial markets of the future.

International experience proves that states and corporations that actively implement innovations in the field of cybersecurity significantly reduce the level of threats and increase their economic resilience. Ukraine is also taking important steps in this direction, integrating digital solutions into the protection of state systems, the banking sector, and the corporate environment.

The first stage. Threat forecasting — this level involves the use of analytical technologies and artificial intelligence to identify potential risks:

Monitoring of markets and economic data (indicators of financial crises, currency manipulation, stock market fraud).

Analysis of big data to detect anomalous transactions, illegal capital flows.

Early detection of cyberattacks using behavioral models.

World experience: In the US, financial regulators (e.g., SEC, Federal Reserve System) use big data analytics to detect market manipulation.

The second stage. Prevention and preventive measures — preventing cyber threats is a critical component of the model:

Implementation of the Zero Trust concept in all financial and government institutions.

Development of cryptographic technologies for secure data storage and transmission.

International cooperation — exchange of intelligence data between countries to combat financial terrorism.

In the EU, the NIS2 (Network and Information Security Directive) regulation requires companies to develop strategies for responding to cyber incidents.

The third stage. Operational response. Includes mechanisms for rapid response to threats:

Cyber threat response centers (CERT, SOC) — their implementation at the level of banks, companies, governments.

Automated fraud prevention platforms — use of AI to block suspicious transactions in real-time.

International blocking of criminal financial operations through SWIFT, FATF, Interpol.

China has a state system for monitoring digital payments, which helps detect and block suspicious financial transactions.

The fourth stage. Analysis and adaptation of strategies. After neutralizing threats, it is necessary to update defense mechanisms:

Regular cybersecurity audits of government and corporate systems.

Increasing the level of digital literacy among employees in the banking and public sectors.

Investments in scientific research to develop new defense solutions.

The UK has a National Cybersecurity Center (NCSC), which conducts regular audits of government institutions and businesses.

In the face of modern threats, Ukraine must actively implement international experience: expanding cooperation with the EU and NATO in the field of cybersecurity; implementing a national system for forecasting financial and cyberattacks; enhancing the security of government information resources and payment systems.

The proposed model for countering economic threats in cyberspace is based on international experience and can be adapted to national characteristics. The implementation of artificial intelligence, cryptography, operational response systems, and analytical forecasting mechanisms are key factors in enhancing economic security.

Table 1.7 – Comparative Analysis of Threat Counteraction in Different Countries

<i>Country</i>	<i>Threat Forecasting</i>	<i>Prevention</i>	<i>Response</i>	<i>Analysis and Adaptation</i>
US	AI analytics of financial flows	Strict financial regulations	CERT in every bank	Regular Fed audits
EU	NIS2, GDPR regulations	Use of Zero Trust	Fraud prevention platforms	Expanded cyber education programs
China	Large-scale financial monitoring	State digital cryptography	Strict regulation of digital currencies	Regular business system audits
Ukraine	Implementation of AI in financial analytics	Development of public-private partnerships	CERT-UA and National Cybersecurity Center	Improvement of cyber defense regulation

Ukraine has the opportunity to integrate advanced technologies into the public sector and financial system, which will contribute to strengthening resilience to cyberattacks and financial manipulations. Further investments in cybersecurity, international partnerships, and the development of digital competencies will enable effective responses to the challenges of the modern world.

The further development of economic security depends on close cooperation between government agencies, the private sector, and international partners in the development of new cybersecurity standards and financial monitoring.

Innovations in the field of economic security are key to the stable development of national economies and the international financial system. The use of modern technologies not only protects enterprises and states from threats but also creates a reliable platform for future economic development. Global trends confirm that countries and companies that actively implement innovations gain significant competitive advantages and resilience to the challenges of the digital age.

Risk management in the digital economy: international experience. The modern digital economy faces new challenges that require effective risk management. The global interdependence of markets, the development of technologies, and the growth of cyber threats force states and businesses to adapt their approaches to ensuring economic security. In this context, economic sanctions, the protection of digital business, and cyber diplomacy play a particularly important role.

Economic sanctions are an effective tool for pressuring states, companies, and individuals that violate international norms or pose threats to global security. In the digital economy, such measures may include:

Restrictions on access to technologies — bans on the supply of advanced technological products (e.g., semiconductors, supercomputers, software).

Disconnection from international financial systems — blocking access to SWIFT, prohibiting the use of digital payments in the global economy.

Sanctions against technology companies — restrictions on cooperation with IT corporations that violate human rights or pose a security threat.

The US and the EU have imposed sanctions against China, limiting its access to high-tech chips. This led to a 20% reduction in semiconductor production in China in 2023.

Restrictions on cooperation with Chinese AI companies — the US and the EU have banned the use of some Chinese AI products in the public sector due to concerns about data leaks.

Sanctions against TikTok — governments of several countries have restricted the use of the Chinese social network in government institutions due to data security concerns.

Table 1.8 – Events and Economic Impact of Risks in the Digital Economy

<i>Year</i>	<i>Event</i>	<i>Economic Impact</i>
2021	US technology restrictions on Huawei	-12 billion USD in losses
2022	Sanctions on Chinese chips	-20% semiconductor production
2023	TikTok restrictions in the US and EU	Loss of 2.3 million users in the US
2024	Control of AI technologies	Impact on 15% of the AI market in China
2025	Expected expansion of sanctions	Further restrictions in cloud technologies

The digital transformation of the economy creates new threats for businesses and government institutions. The key risks are:

Cyberattacks on financial systems — hacking of banking institutions, cryptocurrency platforms, fraud in financial operations. In 2023, global losses from cyberattacks on the financial sector exceeded \$6 trillion.

Leakage of confidential information — in 2022, data breaches in the banking sector led to losses of \$4.2 billion.

Sabotage in cloud environments — attacks on cloud services increased by 300% over the past five years.

Cyber diplomacy is a branch of diplomacy focused on ensuring international security in cyberspace, developing rules and norms for digital interaction between states, combating cybercrime, and strengthening international cooperation in the field of cybersecurity.

Key Directions of Cyber Diplomacy:

- Development of international cybersecurity standards — harmonization of interstate norms regarding responsible behavior in cyberspace.
- Joint initiatives against cybercrime — exchange of intelligence data, development of common mechanisms for accountability for cyberattacks (*Захаренко К., 2018*).

- Coordination of sanctions and measures in response to cyberattacks — imposition of sanctions against countries or entities that engage in malicious activities in cyberspace.
- Regulation of cryptocurrencies and digital assets — formation of international standards for controlling financial flows in the digital environment.
- Development of cyber peacekeeping mechanisms — joint initiatives to avoid cyber conflicts between countries.

Table 1.9 – World Examples of Cyber Diplomacy (2021-2025)

<i>Year</i>	<i>Event</i>	<i>Participating Countries</i>	<i>Impact</i>
2021	Creation of the UN International Cybersecurity Forum	193 UN member states	Formation of global cybersecurity norms
2022	EU introduces the Cyber Diplomacy Tool	EU countrie	Possibility of imposing sanctions for cyberattacks
2023	G7 adopts a joint cyber pact to protect critical infrastructure	US, Canada, Japan, EU	Strengthening cybersecurity of energy and financial sectors
2024	US and EU sign a digital resilience agreement	US, EU	Coordination of cybersecurity measures against external threats
2025	Expected expansion of NATO in the field of cybersecurity	NATO countries	Deepening cooperation in cyber defense

The European Union is actively developing cyber diplomacy through the PESCO program, which promotes joint projects in the field of cyber defense.

In 2023, the Ministry of Foreign Affairs of Ukraine established a cyber diplomacy department to coordinate international cooperation in the field of digital security.

The UN continues to work on global norms of behavior in cyberspace aimed at preventing cyber conflicts.

The G7 is developing mechanisms for responding to global cyber threats, particularly in the protection of financial and energy infrastructure.

Challenges of Cyber Diplomacy

Development of technologies and the emergence of new threats — the constant development of artificial intelligence, quantum computing, and cyber weapons requires the adaptation of diplomatic strategies.

Lack of universal international norms — there is still no unified international legislation on accountability for cybercrimes and cyberattacks.

Increase in the number of state and private cyber operations — some countries are developing strategies for active cyber defense, which could lead to an increase in cyber conflicts.

Regulation of cryptocurrencies — the issue of controlling digital finances remains one of the key challenges for international relations.

International cooperation against cyber terrorism — joint efforts to combat the use of cyberspace for financing terrorist organizations and influencing the international economy.

Cyber diplomacy is an integral part of modern international politics. Thanks to joint initiatives, international norms, and the coordination of efforts between states, it is possible to significantly reduce the risks of digital conflicts and increase the level of protection of the global economy.

The further development of cyber diplomacy depends on the ability of the international community to quickly adapt to changes in technologies and threats arising in the digital space.

Therefore, the establishment of international cybersecurity norms is a key task for the UN, G7, EU, and NATO. Cyber diplomacy is becoming an important tool for preventing cyber conflicts and developing cyber defense mechanisms. Cooperation in the field of digital security between the US, EU, NATO, and Ukraine is strengthening, contributing to stability in the digital environment. The challenges of cyber diplomacy require innovative approaches and constant updating of international legislation.

To ensure effective risk management in the digital economy, states use international and national standards. The main norms and regulations are presented in Table 1.10.

Table 1.10 – International and National Standards

<i>Standard / Norm</i>	<i>Description</i>	<i>Countries / Organizations</i>
ISO 31000:2018	Risk management, principles and guidelines for organizations	Global standard (ISO)
ISO/IEC 27001:2013	Information security management system, minimization of cyber threat risks	Global standard (ISO)
ISO/IEC 27005	Guidelines for managing information security risks	Global standard (ISO)
NIST Cybersecurity Framework	Cybersecurity risk management for enterprises and the public sector	US (NIST)
GDPR (General Data Protection Regulation)	Regulation on the protection of user data, minimization of information leakage risks	EU
DORA (Digital Operational Resilience Act)	Regulation on the digital resilience of the financial sector, risk control	EU
NIS2 Directive	Cybersecurity directive for critical infrastructure	EU
COSO ERM (Enterprise Risk Management)	Integrated risk management, implementation of strategies for financial institutions	US
PCI DSS (Payment Card Industry Data Security Standard)	Protection of payment card transactions, management of financial data risks	US, EU, international financial organizations
CPS 234 (APRA Standard)	Requirements for information security of financial institutions	Australia
MAS TRM (Technology Risk Management)	Management of technological risks in the financial sector	Singapore
Basel III	Regulation of banking risks, capital requirements	Global standard (Basel Committee)

These standards ensure consistent approaches to risk management in the digital economy and help organizations adapt to modern threats. The further development of the regulatory framework will depend on new technological challenges and international cooperation in the field of digital security.

Next, we present a mathematical model of risk management in the digital economy described in Python. To execute and view the results, it is necessary to use one of the following programs or development environments:

Programs for running the code:

Jupyter Notebook — an interactive environment for executing Python code, convenient for working with data analysis.

Google Colab — a free online service that supports Python, allowing you to run code without installing additional software.

VS Code (with the Python extension installed) — a powerful code editor that supports visualization and data processing.

PyCharm — a development environment focused on Python, suitable for complex analytical projects.

Anaconda (Spyder) — a scientific-analytical environment for working with Python, containing all the necessary libraries.

Libraries used in the code:

NumPy — for working with numerical arrays and calculations.

Pandas — for processing and analyzing data in the form of tables.

Matplotlib — for data visualization (graphs and charts).

How to view and run the model? If using Jupyter Notebook or Google Colab: Copy the code into a new notebook (file with .ipynb extension).

Execute the code in the cells one by one. Get the results in the form of a risk table and a risk change graph.

If using VS Code or PyCharm: Create a new .py file and paste the code. Install the necessary libraries by running the commands: `pip install numpy pandas matplotlib` and execute the code using the Python environment.

The table with risk calculations will be available as a DataFrame object.

The graph will show the dynamics of the overall risk level over the selected time period. The code is provided below:

```
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt

# Parameters of the digital economy risk model
factors = {
    'Cyber Threats': 0.3,
    'Financial Stability': 0.25,
    'Automation': 0.2,
    'Regulatory Environment': 0.15,
    'Globalization': 0.1
}

# Data for assessing the impact of risks on the economy (hypothetical values)
years = np.arange(2020, 2030)
risk_values = {
```

```

'Cyber Threats': np.random.uniform(0.5, 1.0, len(years)),
'Financial Stability': np.random.uniform(0.3, 0.8, len(years)),
'Automation': np.random.uniform(0.4, 0.9, len(years)),
'Regulatory Environment': np.random.uniform(0.2, 0.7, len(years)),
'Globalization': np.random.uniform(0.1, 0.6, len(years))
}

# Calculation of the weighted risk level
risk_index = np.zeros(len(years))
for factor, weight in factors.items():
    risk_index += np.array(risk_values[factor]) * weight

# Creating a risk table
risk_df = pd.DataFrame(risk_values, index=years)
risk_df['Overall Risk Level'] = risk_index

# Visualization of the risk level
plt.figure(figsize=(10, 5))
plt.plot(years, risk_index, marker='o', linestyle='-', label='Overall Risk Level')
plt.xlabel('Year')
plt.ylabel('Risk Level')
plt.title('Risk Management Model in the Digital Economy')
plt.legend()
plt.grid(True)
plt.show()

# Output of the risk table
risk_df

```

Mathematical model of risk management in the digital economy. The formula for calculating the overall risk level:

$$R(t) = \sum (W_i * F_i(t)) \quad (1.1)$$

where:

- R(t) – overall risk level in year t,
- W_i – weight of the i-th risk factor,
- F_i(t) – value of the i-th risk factor in year t,
- Σ – sum over all risk factors.

The key influencing factors identified by experts and their significance are listed below. The indicators are set depending on the situation and factors that directly affect the systems:

- Cyber Threats (W₁=0.3)
- Financial Stability (W₂=0.25)
- Automation (W₃=0.2)
- Regulatory Environment (W₄=0.15)
- Globalization (W₅=0.1)

Let's calculate the situation in Ukraine and the world based on our model.

Table 1.11 – Risk Level in the Digital Economy (Ukraine and the World)

<i>Year</i>	<i>Overall Risk Level (Ukraine)</i>	<i>Overall Risk Level (World)</i>
2024	0,605	0,7050000000000001
2025	0,625	0,7250000000000001

An example of the application of a mathematical model of risk management in the digital economy, taking into account current indicators for Ukraine and the world in 2024-2025.

Analysis of the Obtained Data.

In Ukraine, the high level of cyber threats (0.9 in 2024 and 0.85 in 2025) is due to active hacker attacks and military cyber operations, relatively low financial stability (0.5 → 0.55), although international aid is improving. Automation is growing (0.6 → 0.65), especially in the field of digital services and IT. The regulatory environment is improving (0.4 → 0.45), which is associated with adaptation to EU standards.

The overall risk level is 0.605 in 2024, decreasing to 0.625 in 2025 due to improved financial situation.

In the world, cyber threats also remain significant (0.75 → 0.7), with ongoing global attacks on critical infrastructure (*A. Kapiton, 2021*). Higher financial stability (0.7 → 0.75) due to market stabilization after the pandemic and crisis. Active automation and implementation of AI (0.8 → 0.85). The regulatory environment is improving through the implementation of new digital laws in the EU and the US (0.6 → 0.65). The overall risk level is 0.705 in 2024, decreasing to 0.725 in 2025, demonstrating stable control over economic challenges.

The formula ensures the assessment of the overall risk level based on weighted values of the main factors.

Risk management in the digital economy requires a comprehensive approach, including economic sanctions, strengthening cybersecurity, and international coordination. Global trends indicate increased control over digital finance, expansion of sanctions mechanisms, and the implementation of new security standards.

Sanctions and technological blockades have a significant economic impact, as evidenced by real cases in China and Huawei. Innovative methods of cyber defense, such as Zero Trust and AI, significantly reduce the risks of financial losses. Cyber diplomacy is becoming an important tool for coordinating between states to maintain the stability of the digital economy.

Conclusions and Development Prospects. Innovative technologies such as artificial intelligence, blockchain, quantum encryption, and Zero Trust are becoming the foundation of digital economic protection. The use of these mechanisms allows minimizing the risks of cyberattacks, preventing financial crimes, and increasing the transparency of economic processes.

Digital technologies are changing the structure of international financial markets. The implementation of central bank digital currencies (CBDCs), automated financial analysis algorithms, and smart contracts creates new opportunities but also brings new threats. An important part of global security is the regulation of the technology sector and international cooperation in combating cyberattacks on financial systems.

The widespread adoption of digital technologies such as artificial intelligence, blockchain, cloud computing, and quantum cryptography is transforming economic processes, increasing their efficiency, but also creating new threats. In particular, the growth of cybercrime, cyberattacks on financial institutions, and manipulation of digital assets require the development of comprehensive cybersecurity strategies.

The overall level of risks in the digital economy varies significantly depending on the level of digitalization, infrastructure development, and legislative regulation. In Ukraine,

cyber threats remain one of the most critical factors affecting financial stability, necessitating investments in cybersecurity and the development of digital defense mechanisms. While global financial markets are adapting to digital challenges, the integration of state digital currencies (CBDCs) could significantly change the international balance of economic relations.

The implementation of innovative information systems ensures an increase in the level of economic security, reducing the risks of fraud and financial manipulations.

Key mechanisms of cyber defense include the use of AI risk analysis, blockchain technologies for transaction protection, and automated financial monitoring systems.

The use of international cybersecurity standards such as GDPR, NIS2, and ISO/IEC 27001 increases the level of protection of the digital economy.

The introduction of the digital hryvnia could significantly change Ukraine's financial system, reducing the level of cash transactions and improving control over financial flows.

Strengthening cyber diplomacy and international cooperation in the field of financial security will reduce the risks of cybercrime and digital sabotage.

Recommendations for the Integration of Information Systems to Strengthen Economic Stability:

- Harmonization of international cybersecurity standards — implementation of unified rules for the protection of financial operations.
- Application of cloud technologies and artificial intelligence — creation of distributed systems for the protection of economic infrastructure.
- Development of an international system for responding to cyber threats — coordination between states for the rapid detection and neutralization of threats.
- Formation of a digital trust policy — expansion of certification and standardization programs for secure technologies in the public and private sectors.
- Strengthening cyber education and training of specialists — development of educational programs for information security and digital finance specialists.

The further development of the digital economy and cybersecurity depends on effective international cooperation, innovative approaches to protecting financial markets, and the integration of advanced technologies into the field of risk management.

In general, information technologies are an important tool for ensuring economic security and the stability of the financial system. For the further development of the digital economy, it is necessary to activate government initiatives in cybersecurity, expand the use of artificial intelligence for threat analysis, and improve the legal framework for digital financial regulation. The implementation of these measures will contribute to the creation of a secure digital environment and ensure the resilience of the economic system in the face of global changes.

References:

- Безпека для мільйонів: українські ІТ-компанії встановили правила використання ІІІ в інноваційних продуктах. <https://surl.li/fzqfdd>
- Біленчук П. Д., Борисова Л. В., Неклонський І. М., Собина В. О. Правові засади інформаційної безпеки України: монографія. Харків, 2018. 289 с. <http://repositc.nuczu.edu.ua/handle/123456789/18077>.

- Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). Вісн. Харк. нац. ун-ту ім. В. Н. Каразіна. 2020. Вип. 29. Серія: Право. С. 281-288. <https://surl.li/oqvawx>
- Грабар І. Г., Гришук Р. В., Молодецька К. В. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія; за заг. ред. Р. В. Гришука. Житомир: ЖНАЕУ, 2019. 280 с. <http://ir.polissiauniver.edu.ua/handle/123456789/9581>.
- Гуз А. М., Ткачук Т. Ю. Досвід України у формуванні національних надбань в інформаційній сфері. Юрид. наук. електр. журн. 2020. № 6. С. 129-133. <https://doi.org/10.32782/2524-0374/2020-6/31>.
- Дубницький В. І., Науменко Н. Ю. Методологічне забезпечення формування інформаційної безпеки в сфері економічної безпеки регіону. Вісник економічної науки України. 2019. № 1 (36). С. 35-39. <https://surl.li/pgaugr>
- ЕП збирала на інвестиційному форумі бізнес, владу та фінансистів: про що говорили. <https://surl.li/yatkra>
- Єврокомісарка з розширення прогнозує відкриття 1-го переговорного кластера з Україною у квітні-травні-2025. <https://interfax.com.ua/news/general/1031277.html>.
- Захаренко К. Теоретичні засади дослідження інформаційної безпеки. Міжнародні відносини, суспільні комунікації та регіональні студії. 2018. № 2 (4). С. 107-116. <https://doi.org/10.29038/2524-2679-2018-02-107-116>.
- Кольцова І. Інформаційна глобалізація в Україні: детермінанти, особливості та перспективи. Міжнародні відносини, суспільні комунікації та регіональні студії. 2018. № 1 (3). С. 43-48. <https://doi.org/10.29038/2524-2679-2018-01-43-48>.
- Комітет з питань інтеграції України до ЄС провів спеціальне засідання щодо скринінгу відповідності законодавства України праву ЄС. https://www.rada.gov.ua/news/news_kom/255661.html.
- Мільярди надходжень у бюджет: Федоров розкрив потенціал легалізації ринку криптовалют. <https://surl.li/tomqhm>
- Про внесення змін до деяких законів України щодо врегулювання окремих питань у сфері електронних комунікацій : Проект Закону № 12094 від 04.10.2024. <https://itd.rada.gov.ua/billinfo/Bills/Card/44975>.
- Про внесення змін до Закону України «Про засади державної регіональної політики» щодо створення Єдиної державної цифрової системи відновлення та розвитку України : Проект Закону № 12154 від 28.10.2024. <https://surl.li/cdbhjl>
- Про внесення змін до статті 115 Закону України «Про електронні комунікації» (щодо сприяння у забезпеченні сталого функціонування електронних комунікаційних мереж та надання електронних комунікаційних послуг, а також заборони демонтажу електронних комунікаційних мереж в умовах надзвичайних ситуацій, надзвичайного та воєнного стану) : Проект Закону № 9593 від 20.12.2024. <https://itd.rada.gov.ua/billinfo/Bills/Card/45111>.
- Про затвердження Порядку проведення первинної оцінки стану імплементації актів права Європейського Союзу (acquis ЄС): Постанова Кабінету Міністрів України від 28.02.2023 № 189. <https://surl.li/rfbthu>
- У Києві відкрили другий у світі Global Government Technology Centre. <https://surl.li/zhcao>
- Ханін І. Г. Формування в міжнародній системі інформаційної безпеки: економічні орієнтири для України. Ефективна економіка. 2015. № 4. <http://www.economy.nayka.com.ua/?op=1&z=4457>.
- Цифровізація містобудування: в Україні створюють Містобудівний кадастр. <https://surl.li/ccvfeayf>
- Як побудувати успішну кар'єру у веб3: новий освітній серіал на Дія.Освіта. <https://surl.li/qoodxo>
- Dwivedi Yogesh K., Hughes D. Laurie, Coombs Crispin, Constantiou Ioanna, Duan Yanqing, Edwards John S. et al. Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. IJIM. 2020. Vol. 55. <https://doi.org/10.1016/j.ijinfomgt.2020.102211>.
- ISO/IEC 27001. Information Security Management. <https://surl.li/aahejt>
- 15 000 євро на розвиток бізнесу: фінал програми Impact Business Accelerator 2024. <https://surl.li/ulmgiv>

- 15 мільярдів гривень у державний бюджет: який потенціал має легалізація криптоактивів в Україні – дослідження. <https://surl.li/jrtlcp>
- European Commission's Initiative on Web 4.0 and Virtual Worlds: a head start in the next technological transition. <https://surl.li/sdullg>
- GTA UA: п'ять IT-компаній об'єдналися в GovTech Альянс України. <https://dou.ua/lenta/news/about-gta-ua/>.
- Soomro Zahoor Ahmed, Shah Mahmood Hussain, Ahmed Javed. Information security management needs more holistic approach: A literature review. <https://doi.org/10.1016/j.ijinfomgt.2015.11.009>.
- The Global Risks Report 2021. The 16th edition of the World Economic Forum's Global Risks. <https://surl.li/idzzez>
- Systematic approach application to the development for the site of university scientific activity / A. Kapiton, O. Diachenko, R. Zakharov, T. Yanchuk // *Системи управління, навігації та зв'язку*. 2021. Вип. 4. С. 52-54. <https://doi.org/10.26906/SUNZ.2021.4.052>.
- Levchenko N., Yanchuk T. (2024). STRATEGY FOR INCREASING THE COMPETITIVENESS OF THE TESLA ELECTRIC VEHICLE/ *Three Seas Economic Journal* , 5 (2), 7-13. <https://doi.org/10.30525/2661-5150/2024-2-2>.
- International scientific symposium: "Wissenschaft und Bildung als Basis für die Modernisierung der Weltordnung / Science and education as the basis for the modernization of the world order", December, 2024, Karlsruhe, Germany. <https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/44449/173019.pdf>.

CHAPTER 8. REGULATION OF INNOVATIVE DEVELOPMENT OF THE AGRARIAN SECTOR OF THE ECONOMY OF UKRAINE

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

Odesa Law Academy National University

(210, Kharkiv highway, Kyiv, 02121, Ukraine)

n.diachenko@ukr.net

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

Abstract. Methods of regulating the innovative development of the agrarian sector of the economy of Ukraine have been studied. It has been established that the agrarian sector is one of the key sectors of the economy of Ukraine, which has a significant impact on the development and well-being of the country, as it combines the production, processing and sale of agricultural products, providing the country's population with food, as well as providing significant export potential. The components of the mechanism for regulating the innovative development of the agrarian sector of the economy of Ukraine have been identified. It has been emphasized that among the methods that can contribute to increasing the efficiency of regulating the innovative development of the agrarian sector of Ukraine, it is advisable to single out the introduction of modern technologies, including precision manufacturing. The advantages of precision manufacturing have been identified. It has been substantiated that automation, robotization and digitalization of processes are key factors in ensuring the efficiency of regulating the innovative development of the agricultural sector. The advantages of automation, robotization of the agricultural sector and the advantages of digitalization of the agricultural sector of the economy of Ukraine have been identified, including: increasing production efficiency, improving product quality, reducing negative impact on the environment, and developing rural areas. It was stated that when implementing digital technologies, it is worth considering the challenges of digitalization of the agricultural sector of the economy of Ukraine, including the problems of cybersecurity and data protection. It was found that organic production in Ukraine is experiencing a period of active development, and the expansion of the range of organic products is one of the key trends in this process. The state, trends, prospects and challenges of organic production in Ukraine are identified. It is emphasized that the successful implementation of innovative regulatory mechanisms in the agricultural sector of the economy of Ukraine is the key to its sustainable development and ensuring competitiveness in the global market.

Keywords: agricultural sector, innovative development, precision manufacturing, public-private partnership, competitiveness.

РЕГУЛЮВАННЯ ІННОВАЦІЙНОГО РОЗВИТКУ АГРАРНОГО СЕКТОРУ ЕКОНОМІКИ УКРАЇНИ

Анотація. Досліджено методи регулювання інноваційного розвитку аграрного сектору економіки України. Встановлено, що аграрний сектор є однією з ключових галузей

економіки України, що має значний вплив на розвиток та добробут країни, адже поєднує в собі виробництво, переробку та реалізацію сільськогосподарської продукції, забезпечуючи населення країни продовольством, а також забезпечуючи значний експортний потенціал. Ідентифіковано складові механізми регулювання інноваційного розвитку аграрного сектору економіки України. Наголошено, що серед методів, які можуть сприяти підвищенню ефективності регулювання інноваційного розвитку аграрного сектору України доцільно виокремити впровадження сучасних технологій, серед яких точне виробництво. Ідентифіковано переваги точного виробництва. Обґрунтовано, що автоматизація, роботизація та цифровізація процесів є ключовими чинниками забезпечення ефективності регулювання інноваційного розвитку аграрної сфери. Ідентифіковано переваги автоматизації роботизації аграрного сектора та переваги цифровізації аграрного сектору економіки України, серед яких: підвищення ефективності виробництва, покращення якості продукції, зменшення негативного впливу на довкілля, розвиток сільських територій. Констатовано, що при впровадженні цифрових технологій варто враховувати виклики цифровізації аграрного сектору економіки України, серед яких проблеми кібербезпеки та захисту даних. Виявлено, що органічне виробництво в Україні переживає період активного розвитку, розширення асортименту органічної продукції є однією з ключових тенденцій цього процесу. Ідентифіковано стан, тенденції, перспективи та виклики органічного виробництва в Україні. Наголошено, що успішне впровадження інноваційних механізмів регулювання в аграрному секторі економіки України є запорукою його сталого розвитку та забезпечення конкурентоспроможності на світовому ринку.

Ключові слова: аграрний сектор, інноваційний розвиток, точне виробництво, державно-приватне партнерство, конкурентоспроможність.

Вступ. Аграрний сектор є однією з ключових галузей економіки України, що має значний вплив на розвиток та добробут країни. Він поєднує в собі виробництво, переробку та реалізацію сільськогосподарської продукції, забезпечуючи населення країни продовольством, а також забезпечуючи значний експортний потенціал. Україна володіє значними площами родючих земель, що є основою для розвитку аграрного сектора економіки. Чорноземи, що займають значну частину території країни, є одними з найродючіших у світі. Розвиток тваринництва представлений розведенням великої рогатої худоби, свиней, птиці та інших видів тварин. Продукція тваринництва забезпечує потреби населення у м'ясі, молоці та інших продуктах. Галузь рослинництва спеціалізується на вирощуванні зернових культур (пшениця, кукурудза, ячмінь), олійних культур (соняшник, ріпак), технічних культур (цукровий буряк, льон), картоплі та овочів. Україна є одним зі світових лідерів з експорту зернових та олійних культур. Аграрний сектор включає в себе також переробні підприємства, що займаються виробництвом харчових продуктів, таких як хлібобулочні вироби, молочна продукція, м'ясні вироби, олія, цукор та інші. Аграрний сектор забезпечує населення країни необхідними продуктами харчування, сприяючи зміцненню продовольчої безпеки та традиційно має значний обсяг експорту зернових, олійних та інших видів продукції.

Постановка проблеми. Ефективність аграрного сектора значною мірою залежить від погодних умов, що може призводити до коливань урожайності та виробництва, а відтак, з метою забезпечення конкурентоспроможності, аграрному сектору для отримання інвестицій на модернізацію виробництва, впровадження новітніх технологій та розвитку інфраструктури необхідно формування сприятливого

інвестиційного клімату. значних інвестицій для. Незважаючи на існуючі проблеми та сучасні виклики, аграрний сектор України має значний потенціал для подальшого розвитку та зростання. За умови ефективного управління, залучення інвестицій та впровадження інновацій, він може стати ще більш важливим чинником економічного розвитку країни та формування продовольчої безпеки України.

Аналіз останніх досліджень та публікацій. Дослідженню особливостей формування засад сталого розвитку аграрного сектора економіки України приділили увагу багато науковців., зокрема виявлено особливості трансформації логістичних зв'язків та економічна ефективність підприємств зернової продукції (Василина О., Попадинець Н., Яхно Т., Садура О., Кравчик Ю., 2024), окреслено механізм впливу сільськогосподарської кооперації на розвиток людського капіталу сільських територій України (Демченко О., 2024), ідентифіковано механізми бюджетного та позабюджетного інвестування (Драган І., Дацій Н., Антонова Л., 2024), виявлено критерії привабливості ринку органічної продукції України (Драган І., Дацій Н., Антонова Л., 2024).

Метою дослідження є ідентифікація механізмів забезпечення ефективності регулювання інноваційного розвитку аграрного сектору економіки України.

Методи забезпечення ефективності регулювання інноваційного розвитку аграрного сектору економіки України.

Аграрний сектор економіки України має значний потенціал для розвитку та забезпечення продовольчої безпеки країни. Проте, для досягнення цієї мети необхідно забезпечити його конкурентоспроможність на ендегенному та екзогенному ринках.

Серед методів, які можуть сприяти підвищенню ефективності регулювання інноваційного розвитку аграрного сектору України доцільно виокремити впровадження сучасних технологій, серед яких *точне виробництво*.

Точне землеробство, як один з сучасних сучасний підходів до ведення сільського господарства, базується на використанні передових технологій для отримання детальної інформації про стан ґрунту, посівів та інших параметрів. Цей підхід дозволяє оптимізувати використання ресурсів, підвищити врожайність та зменшити негативний вплив на довкілля.

Однією з базових сучасних технологій, які використовуються в точному землеробстві є GPS-навігація. Упровадження GPS-навігація дозволяє точно визначати місцезнаходження сільськогосподарської техніки на полі, що забезпечує точне виконання технологічних операцій, таких як посів, обробка ґрунту, внесення добрив та засобів захисту рослин.

Використання безпілотних літальних апаратів з метою отримання аерофотознімків високої роздільної здатності, дозволяє створювати детальні карти полів, оцінювати стан посівів, виявляти проблемні ділянки та оперативно приймати рішення щодо обробки ґрунту та внесення добрив.

Для збору даних про стан ґрунту, рослин та інших параметрів використовуються сучасні *сенсори* – електронні пристрої, що складаються з трьох основних компонентів: датчика, чутливого до змін фізичних показників елемента, який перетворює їх на електричний сигнал; процесора, який оцифровує цей сигнал; інтерфейсу, який передає ці дані в пристрій, що використовує цей сенсор. Існують різні типи сенсорів, які можуть вимірювати вологість ґрунту, вміст поживних речовин, температуру, освітленість та інші параметри.

Системи управління даними дозволяють збирати, обробляти та аналізувати дані, отримані з різних джерел, таких як дрони, GPS-навігація, сенсори та інші. Ці системи допомагають приймати обґрунтовані рішення щодо управління сільськогосподарським виробництвом.

- Серед переваг точного землеробства (табл. 1) доцільно виокремити використання дронів, GPS-навігації, сенсорів та інших технологій, що дозволяють:
- отримувати детальну інформацію про стан ґрунту, посівів та інших параметрів, що дозволяє оптимізувати використання ресурсів та підвищити врожайність;
 - зменшити витрати;
 - знизити негативний вплив на довкілля;
 - покращити якість продукції.

Таблиця 1. Переваги точного землеробства

№	Напрямок	Характеристика
1.	Підвищення врожайності	За рахунок оптимізації використання ресурсів та точного виконання технологічних операцій, точне землеробство дозволяє підвищити врожайність сільськогосподарських культур
2.	Зменшення витрат	Точне землеробство дозволяє зменшити витрати на добрива, засоби захисту рослин, воду та інші ресурси за рахунок їх більш ефективного використання
3.	Зниження негативного впливу на довкілля	За рахунок зменшення використання хімічних речовин та більш ефективного використання ресурсів, точне землеробство сприяє зниженню негативного впливу на довкілля, зокрема й шляхом формування системи управління відходами (Карбовська, 2024).
4.	Покращення якості продукції	Точне землеробство дозволяє отримувати більш якісну сільськогосподарську продукцію за рахунок забезпечення оптимальних умов для росту і розвитку рослин

В Україні точне землеробство знаходиться на етапі активного розвитку. Все більше суб’єктів господарювання починають використовувати сучасні технології для підвищення ефективності свого виробництва.

- Проте, для широкого впровадження точного землеробства необхідно вирішити ряд проблем, таких:
- висока вартість обладнання;
 - неперервна необхідність навчання персоналу;
 - розвиток інфраструктури.

Точне землеробство має великий потенціал для розвитку в Україні. За рахунок використання сучасних технологій, українські суб’єкти господарювання можуть підвищити свою конкурентоспроможність на ендегенному та екзогенному ринках, забезпечити продовольчу безпеку країни та зменшити негативний вплив на довкілля.

Автоматизація та роботизація є ключовими чинниками підвищення ефективності регулювання інноваційного розвитку аграрної сфери.

Цифровізація процесів автоматизації в аграрному секторі економіки України є ключовим чинником підвищення ефективності, продуктивності та конкурентоспро-

можності галузі.

Вона охоплює широкий спектр технологій та інструментів, які можуть бути застосовані на різних етапах управління та виробничого циклу – від посіву до збору врожаю та його реалізації.

Застосування сучасних технологій дозволяє оптимізувати виробничі процеси, зменшити витрати та підвищити ефективність господарювання (табл. 2).

Таблиця 2. Переваги автоматизації та роботизації в аграрному секторі

№	Напрямок	Характеристика
1.	Підвищення продуктивності	Автоматизовані системи та роботи здатні виконувати роботи швидше та точніше, ніж люди. Це призводить до збільшення обсягів виробництва та підвищення врожайності
2.	Зниження витрат	Використання роботів та автоматизованих систем дозволяє зменшити витрати на оплату праці, матеріали та енергоресурси
3.	Покращення якості продукції	Автоматизація забезпечує точне дотримання технологічних процесів, що сприяє підвищенню якості сільськогосподарської продукції
4.	Оптимізація використання ресурсів	Автоматизовані системи дозволяють більш ефективно використовувати воду, добрива та інші ресурси, що зменшує негативний вплив на довкілля
5.	Покращення умов праці	Автоматизація та роботизація дозволяють зменшити фізичне навантаження на працівників та зробити їх працю більш безпечною та комфортною

Базовими напрямками впровадження автоматизації та роботизації в аграрному секторі економіки України є рослинництво, тваринництво, переробка сільськогосподарської продукції (рис. 1):

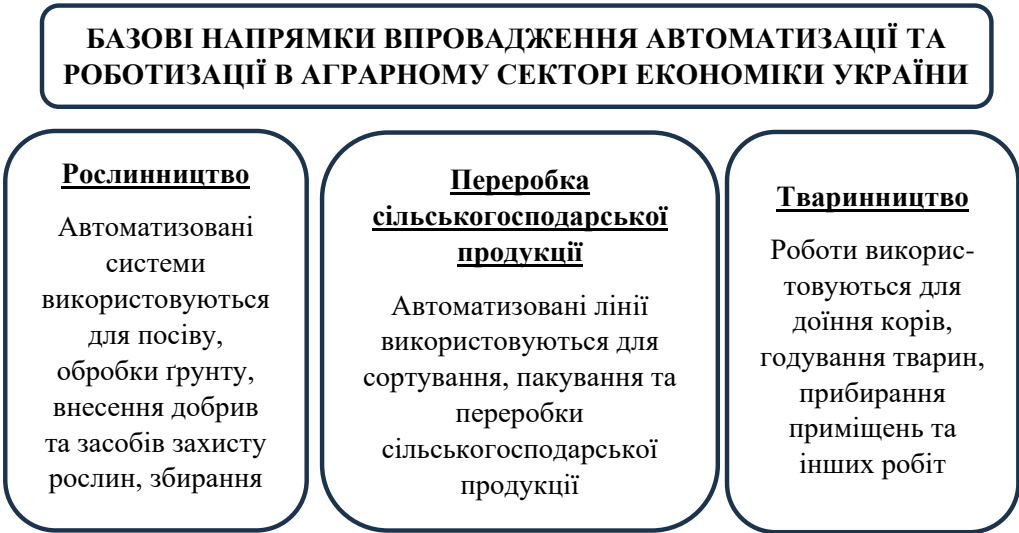


Рис. 1. Базові напрямки впровадження автоматизації та роботизації в аграрному секторі економіки України

Цифрові платформи для управління господарством в аграрному секторі економіки України використовують при:

- створенні комплексних систем управління господарством, які об'єднують дані з різних джерел та дозволяють ефективно планувати, контролювати та аналізувати всі аспекти діяльності підприємства;
- використанні хмарних технологій для зберігання та обробки даних, а також для забезпечення доступу до інформації з будь-якого місця та пристрою;
- упровадженні систем підтримки прийняття рішень на основі аналізу даних та прогнозів.

Інструменти Інтернету речей (IoT) в аграрному секторі застосовують при необхідності:

- встановлення датчиків на сільськогосподарській техніці, обладнанні та полях для збору даних про стан ґрунту, погодних умов, росту рослин та інших параметрів;
- передачі даних через інтернет для подальшого аналізу та використання для прийняття рішень;
- дистанційного керування обладнанням та системами.

Серед проблем і перспектив впровадження автоматизації та роботизації в аграрній сфері доцільно виокремити:

- високу вартість обладнання, з урахуванням чого з метою впровадження автоматизованих систем та роботів необхідно інтенсифікувати інвестиційні процеси;
- необхідність навчання персоналу обслуговуванню технічних засобів та роботі з сучасним обладнанням.
- потребу розвитку інфраструктури, зокрема, доступ до Інтернету та електроенергії.

Завдяки впровадженню сучасних технологій, українські суб'єкти господарювання можуть підвищити свою конкурентоспроможність на ендегенному та екзогенному ринках, забезпечити продовольчу безпеку країни та зменшити негативний вплив на довкілля.

Серед переваги цифровізації аграрного сектору економіки України доцільно виокремити: підвищення ефективності виробництва, покращення якості продукції, зменшення негативного впливу на довкілля, розвиток сільських територій (табл. 3).

При впровадженні цифрових технологій варто враховувати виклики цифровізації аграрного сектору економіки України, серед яких проблеми кібербезпеки та захисту даних (Юрчук, 2024).

Штучний інтелект має потенціал стати ключовим чинником підвищення ефективності регулювання інноваційного розвитку аграрного сектору України. Застосування штучного інтелекту в аграрній сфері може допомогти вирішити багато проблем, з якими стикається галузь, та відкрити нові можливості для розвитку.

Серед інноваційних методів, які можуть сприяти підвищенню ефективності регулювання інноваційного розвитку аграрного сектору України доцільно виокремити розвиток органічного виробництва.

Уряд України розробив та впроваджує програми підтримки органічного виробництва (Сичук, 2024).

Серед перспектив органічного виробництва доцільно виокремити:

- Європейський зелений курс та прагнення України відповідати вимогам ЄС

щодо екологічно чистого виробництва сприяє розвитку органічного сектору.

– Зростаючий попит на органічну продукцію в світі та в Україні.

Таблиця 3. Переваги цифровізації аграрного сектору економіки України

Напрямок	Характеристика	Опис
Підвищення ефективності виробництва	<i>Управління діяльністю:</i>	Цифрові платформи та інструменти для управління сільськогосподарським виробництвом, обліку ресурсів, аналізу даних та прийняття рішень дозволяють підвищити ефективність управління та знизити ризики.
	<i>Точне землеробство</i>	Використання дронів, GPS-навігації, сенсорів та інших технологій дозволяє отримувати детальну інформацію про стан ґрунту, посівів та інших параметрів, що дозволяє оптимізувати використання ресурсів та підвищити врожайність.
	<i>Автоматизація та роботизація</i>	Використання автоматизованих систем та роботів для виконання різних сільськогосподарських робіт, таких як посів, обробка ґрунту, збирання врожаю, дозволяє зменшити витрати на оплату праці та підвищити ефективність виробництва.
Покращення якості продукції	<i>Контроль якості</i>	Використання цифрових технологій дозволяє контролювати якість продукції на всіх етапах виробництва, від посіву до збирання та переробки.
	<i>Відстеження походження</i>	Цифрові системи дозволяють відстежувати походження продукції, що підвищує довіру споживачів та забезпечує можливість ідентифікації та відкликання неякісної продукції.
Зменшення негативного впливу на довкілля	<i>Оптимізація використання ресурсів</i>	Цифрові технології дозволяють більш ефективно використовувати воду, добрива та інші ресурси, що зменшує негативний вплив на довкілля.
	<i>Зменшення використання пестицидів</i>	Точне землеробство дозволяє зменшити використання пестицидів за рахунок їх більш точного та ефективного застосування.
Розвиток сільських територій	<i>Доступ до інформації та знань</i>	Цифрові технології забезпечують доступ до інформації та знань для суб'єктів господарювання, що сприяє підвищенню їх кваліфікації та ефективності роботи.
	<i>Розвиток інфраструктури</i>	Розвиток цифрової інфраструктури в сільських районах сприяє створенню нових робочих місць та розвитку місцевої економіки

Сертифікація органічного виробництва є важливим інструментом для розвитку органічного сільського господарства в Україні та забезпечення споживачів якісною та безпечною продукцією. Вона підтверджує відповідність виробництва

встановленим стандартам органічного виробництва, що гарантує екологічну чистоту продукції та її користь для здоров'я людини.

Переваги сертифікації органічного виробництва:

1. Підвищення довіри споживачів: сертифікат органічного виробництва є гарантією якості та безпеки продукції для споживачів, що сприяє підвищенню довіри до виробника та його продукції.

2. Розширення ринку збуту: органічна продукція має попит як на ендегенному, так і на екзогенному ринках, що відкриває для виробників можливості для розширення ринку збуту та збільшення обсягів продажів.

3. Збільшення прибутку: органічна продукція, як правило, має вищу ціну порівняно зі звичайною продукцією, що дозволяє виробникам отримувати більший прибуток.

4. Покращення іміджу виробника: сертифікація органічного виробництва свідчить про відповідальне ставлення виробника до довкілля та здоров'я споживачів, що сприяє покращенню його іміджу.

Органічне виробництво в Україні переживає період активного розвитку, і розширення асортименту органічної продукції є однією з ключових тенденцій цього процесу. Зростаючий попит на екологічно чисті та безпечні продукти харчування створює сприятливі умови для збільшення різноманітності органічних товарів на ринку.

Незважаючи на позитивні тенденції, розширення асортименту органічної продукції в Україні стикається з низкою викликів, серед яких:

– Обмеженість сировини: виробництво органічної продукції потребує значної кількості органічної сировини, яку не завжди достатньо для задоволення зростаючого попиту.

– Висока вартість виробництва: органічне виробництво потребує більших витрат на дотримання стандартів, сертифікацію та контроль якості, що впливає на собівартість продукції.

– Недостатня інфраструктура: для зберігання, переробки та транспортування органічної продукції необхідна відповідна інфраструктура, яка в Україні ще недостатньо розвинена.

– Маркетинг та збут: виробникам органічної продукції необхідно ефективно просувати свою продукцію на ринку та знаходити канали збуту.

На сьогоднішній день в Україні існують різноманітні канали збуту органічної продукції, серед яких можна виділити:

1. Прямі продажі:

– Гуртова торгівля: організовані спеціально для продажу органічної продукції безпосередньо від виробника до споживача.

– Інтернет-магазини: дозволяють замовляти органічну продукцію онлайн з доставкою додому або в пункт видачі.

– Доставка додому: деякі виробники пропонують послугу доставки органічної продукції безпосередньо додому споживачам.

– Продаж на фермі: споживачі можуть відвідати ферму та придбати органічну продукцію безпосередньо у виробника.

2. Роздрібні мережі:

–Супермаркети: багато супермаркетів мають відділи або полиці з органічною продукцією.

–Спеціалізовані магазини: існують магазини, які спеціалізуються на продажу органічної продукції.

–Еко-магазини: пропонують широкий асортимент екологічно чистих товарів, включаючи органічну продукцію.

3. Оптовий продаж:

– Органічні гуртові бази: закупають органічну продукцію у виробників та продають її роздрібним торговцям.

– Кооперативи: об'єднання виробників для спільного продажу органічної продукції.

4. Експорт:

– Міжнародні ярмарки: участь у міжнародних ярмарках органічної продукції дозволяє виробникам знаходити іноземних партнерів та експортувати свою продукцію.

– Прямі контракти: укладення прямих контрактів з іноземними компаніями на постачання органічної продукції *(Левченко, 2023)*.

Незважаючи на існування різноманітних каналів збуту, органічні виробники в Україні стикаються з низкою проблем, серед яких:

– кількість магазинів, які спеціалізуються на продажу органічної продукції, є недостатньою для задоволення зростаючого попиту;

– органічна продукція, як правило, має вищу ціну порівняно зі звичайною, що може обмежувати її доступність для деяких споживачів;

– здебільшого споживачі не знають про переваги органічної продукції та не вміють її відрізнити від звичайної;

– органічним виробникам доводиться конкурувати зі звичайними виробниками, які пропонують більш дешеву продукцію.

Для вирішення цих проблем та розвитку ефективних каналів збуту органічної продукції необхідні:

– державна підтримка та створення сприятливих умов для відкриття магазинів, які спеціалізуються на продажу органічної продукції.

– оптимізація виробничих процесів, зменшення витрат на логістику та маркетинг дозволить зменшити ціну на органічну продукцію та зробити її більш доступною для споживачів.

– проведення інформаційних кампаній, спрямованих на підвищення обізнаності споживачів про переваги органічної продукції.

– надання грантів, субсидій та інших видів підтримки органічним виробникам сприятиме розвитку органічного виробництва та збільшенню обсягів продукції.

Розвиток ефективних каналів збуту органічної продукції є важливим чинником успіху органічного виробництва в Україні. За умови вирішення існуючих проблем та створення сприятливих умов, органічна продукція зможе зайняти гідне місце на ринку та задовольнити потреби споживачів у якісних та безпечних продуктах харчування.

Створення ефективних каналів збуту органічної продукції, таких як

спеціалізовані магазини, інтернет-магазини, фермерські ринки, дозволяє розширити ринок збуту та збільшити доходи виробників.

Незважаючи на значні переваги, органічне виробництво в Україні стикається з низкою викликів, таких як:

- висока вартість сертифікації;
- недостатня поінформованість споживачів про органічну продукцію;
- конкуренція з боку недобросовісних виробників.

Проте, органічне виробництво має великий потенціал для розвитку в Україні. За підтримки держави, інвесторів та міжнародних партнерів, українські суб'єкти господарювання можуть збільшити обсяги виробництва органічної продукції, що сприятиме розвитку аграрного сектору економіки країни та забезпеченню продовольчої безпеки. Отримання сертифікатів органічного виробництва дозволяє підтвердити якість та екологічність продукції, що підвищує її конкурентоспроможність на ендегенному та екзогенному ринках.

Механізми забезпечення ефективності регулювання інноваційного розвитку аграрного сектору економіки України.

Підтримка малого та середнього бізнесу є базовим механізмом забезпечення ефективності регулювання інноваційного розвитку аграрного сектору економіки України. Малий та середній бізнес відіграє ключову роль у розвитку аграрного сектору економіки України, забезпечуючи значну частину виробництва, переробки та реалізації сільськогосподарської продукції. Підтримка малого та середнього бізнесу є вирішальним чинником підвищення ефективності регулювання інноваційного розвитку аграрного сектору, сприяючи його модернізації, інноваційному розвитку та створенню нових робочих місць.

Підтримка малого та середнього бізнесу є важливою для аграрного сектору, адже:

- малий та середній бізнес є основним джерелом зайнятості в сільській місцевості, сприяючи зменшенню безробіття та відтоку населення з сіл;
- малий та середній бізнес часто є більш гнучкими та відкритими до інновацій, ніж великі підприємства, адже швидше впроваджують нові технології, розробляють нові продукти та послуги, що сприяє модернізації аграрного сектору;
- малий та середній бізнес спеціалізуються на різних видах діяльності, що забезпечує диверсифікацію аграрного виробництва та зменшує залежність від окремих культур або видів продукції;
- розвиток малого та середнього бізнесу сприяє посиленню конкуренції на аграрному ринку, що стимулює підвищення ефективності виробництва та зниження цін для споживачів;
- малий та середній бізнес є основою для розвитку громадянського суспільства та зміцнення соціальної стабільності в сільській місцевості.

Базовими формами підтримки малого та середнього бізнесу в аграрному секторі є:

1. Фінансова підтримка:

- гранти та субсидії на розвиток бізнесу, придбання техніки, впровадження інновацій;
- пільгові кредити для сільськогосподарських виробників;

- програми мікрокредитування для малого бізнесу.
- 2. Інформаційна та консультаційна підтримка:
 - навчальні програми та семінари для суб'єктів господарювання з питань сучасних технологій, управління бізнесом, маркетингу;
 - консультації з питань юридичного оформлення, оподаткування, ведення бухгалтерського обліку;
 - доступ до інформації про ринки збуту, ціни, нові технології.
- 3. Технічна та технологічна підтримка:
 - створення центрів колективного користування технікою та обладнанням;
 - сприяння участі малого та середнього бізнесу у виставках, ярмарках, конференціях;
 - підтримка розвитку органічного виробництва та сертифікації продукції.
- 4. Спрощення регулювання та зменшення адміністративного тиску:
 - скасування зайвих бюрократичних процедур;
 - зменшення кількості перевірок та звітів;
 - спрощення процедури отримання дозволів та ліцензій.
- 5. Розвиток інфраструктури:
 - будівництво та реконструкція доріг, транспортних розв'язок, складських приміщень.
 - забезпечення доступу до Інтернету та інших комунікацій.

Серед успішних проєктів підтримки малого та середнього бізнесу в аграрному секторі варто виокремити:

- Програму «Агро 2.0», яка передбачає надання грантів та субсидій для малих та середніх суб'єктів господарювання.
- Програму «Старт», яка підтримує суб'єктів господарювання та підприємців, які лише починають свій бізнес в аграрному секторі.
- Діяльність сільськогосподарських кооперативів, які об'єднують малих виробників для спільного виробництва та збуту продукції.

Підтримка малого та середнього бізнесу є важливим чинником забезпечення ефективності регулювання інноваційного розвитку аграрного сектору економіки України. Успішний розвиток малого та середнього бізнесу сприяє створенню нових робочих місць, модернізації виробництва, диверсифікації сільськогосподарської діяльності та підвищенню ефективності аграрного сектору в цілому. Для досягнення цих цілей необхідно продовжувати удосконалення державної політики підтримки малого та середнього бізнесу, створювати сприятливі умови для їх розвитку та забезпечувати доступ до фінансових, інформаційних та технічних ресурсів.

Надання грантів та субсидій малим та середнім суб'єктам господарювання на впровадження інновацій, придбання сучасної техніки, розвиток органічного виробництва дозволяє підвищити їх конкурентоспроможність.

В умовах глобалізації та швидкого розвитку технологій, суб'єкти господарювання повинні постійно вдосконалювати свої знання та навички, щоб залишатися конкурентоспроможними та ефективно управляти своїм бізнесом.

Навчальні програми та консультації для суб'єктів господарювання є важливим інструментом для досягнення цієї мети.

Сільське господарство постійно розвивається, поява нових технологій сприяє

підвищенню врожайності, зменшенню витрат та покращенню якості продукції. Суб'єкти господарювання повинні бути обізнані з новими технологіями та вміти їх застосовувати на практиці.

Суб'єкти господарювання повинні вміти планувати свою діяльність, управляти фінансами, маркетингом та іншими аспектами бізнесу.

Суб'єкти господарювання повинні мати навички правильно представити власну продукцію на ринку, визначати цільову аудиторію, розробляти маркетингову стратегію та використовувати різні канали збуту.

З метою набуття суб'єктами господарювання необхідних знань, вмінь та практичних навичок розроблені комплекс форм навчання та консультацій, серед яких:

- тренінги та семінари – короткострокові навчальні заходи, які охоплюють конкретні теми, такі як сучасні технології вирощування культур, управління фермою, маркетинг сільськогосподарської продукції тощо;

- вебінари – онлайн-семінари, які дозволяють суб'єктам господарювання отримувати знання, не виходячи з дому;

- консультації – індивідуальні консультації з експертами з питань сучасних технологій, управління бізнесом, маркетингу тощо;

- навчальні поїздки – поїздки на передові фермерські господарства, де суб'єкти господарювання можуть ознайомитися з сучасними технологіями та передовим досвідом;

- онлайн-платформи – веб-сайти та онлайн-платформи, де суб'єкти господарювання можуть знайти корисну інформацію, навчальні матеріали, відеолекції тощо.

Такі заходи проводять державні установи (Міністерство аграрної політики та продовольства України, обласні та районні управління сільського господарства), навчальні заклади (аграрні університети, коледжі, технікуми), громадські організації (асоціації фермерів, сільськогосподарські кооперативи), міжнародні організації (проекти міжнародної технічної допомоги, які спрямовані на розвиток сільського господарства), приватні компанії, які займаються виробництвом та збутом сільськогосподарської техніки, насіння, добрив тощо.

Навчання та консультації є важливим інструментом для підвищення кваліфікації суб'єктів господарювання та розвитку їх бізнесу. Суб'єкти господарювання повинні постійно вчитися та вдосконалювати свої знання та навички, щоб залишатися конкурентоспроможними.

Держава, навчальні заклади, громадські організації та міжнародні проекти повинні створювати умови для доступу суб'єктів господарювання до якісного та сучасного навчання.

Організація навчальних програм та консультацій для суб'єктів господарювання з питань сучасних технологій, управління бізнесом, маркетингу дозволяє підвищити їх кваліфікацію та ефективність роботи.

Ефективним чинником забезпечення ефективності регулювання інноваційного розвитку аграрного сектору економіки України є кооперація.

Сільськогосподарська кооперація є важливим механізмом підвищення ефективності регулювання інноваційного розвитку аграрного сектору економіки

України. Вона дозволяє малим та середнім сільськогосподарським виробникам об'єднати свої ресурси та зусилля для досягнення спільних цілей, таких як збільшення обсягів виробництва, поліпшення якості продукції, зниження витрат та розширення ринків збуту. Серед переваг сільськогосподарської кооперації варто виокремити:

- збільшення економічної сили: об'єднання в кооперації дозволяє малим виробникам отримати доступ до ресурсів, які їм були б недоступні окремо, таких як кредити, сучасна техніка, технології та інформація;
- покращення якості продукції: спільні зусилля членів кооперації дозволяють підвищити якість продукції за рахунок впровадження сучасних технологій, контролю якості та стандартизації;
- зниження витрат: кооперація дозволяє зменшити витрати на закупівлю матеріалів, техніки, енергоресурсів та інших ресурсів за рахунок оптових закупівель та спільного використання;
- розширення ринків збуту: кооперації мають більші можливості для виходу на нові ринки збуту, як ендегенні, так і екзогенні, за рахунок об'єднання обсягів виробництва та маркетингових зусиль;
- захист інтересів: кооперації представляють інтереси своїх членів у відносинах з іншими учасниками ринку, такими як переробники, торговельні мережі, постачальники ресурсів та органи влади (Демченко, 2024).

В Україні існують різні види сільськогосподарських кооперацій, які можуть займатися різними видами діяльності, такими як:

- виробничі кооперації, які займаються виробництвом сільськогосподарської продукції, її переробкою та збутом;
- обслуговуючі кооперації, що надають послуги з обробки землі, збирання врожаю, зберігання продукції, маркетингу, постачання ресурсів тощо;
- споживчі кооперації закупають товари для потреб членів кооперації, в тому числі сільськогосподарську продукцію.

Для успішного розвитку сільськогосподарської кооперації в Україні необхідно створити сприятливі умови, які передбачають:

- удосконалення законодавства, яке регулює діяльність сільськогосподарських кооперацій, спрощення процедури їх створення та реєстрації;
- надання державної підтримки сільськогосподарським коопераціям у вигляді грантів, субсидій, пільгових кредитів;
- організацію навчальних програм та консультацій для членів кооперацій з питань управління, маркетингу, сучасних технологій тощо;
- забезпечення доступу до інформації про ринки збуту, ціни, нові технології тощо.

Сільськогосподарська кооперація є важливим механізмом підвищення ефективності регулювання інноваційного розвитку аграрного сектору економіки України. Вона дозволяє малим та середнім виробникам об'єднати свої ресурси та зусилля для досягнення спільних цілей, таких як збільшення обсягів виробництва, поліпшення якості продукції, зниження витрат та розширення ринків збуту.

Для успішного розвитку сільськогосподарської кооперації в Україні необхідно створити сприятливі умови, які включають в себе законодавче забезпечення,

фінансову підтримку, освітню та консультаційну підтримку, а також інформаційну підтримку.

Створення сільськогосподарських кооперативів дозволяє малим та середнім підприємствам об'єднати свої ресурси та зусилля для вирішення спільних проблем, таких як закупівля матеріалів, збут продукції, доступ до фінансів.

Ефективним чинником забезпечення ефективності регулювання інноваційного розвитку аграрного сектору економіки України є розвиток інфраструктури.

Інфраструктура включає в себе широкий спектр елементів, таких як транспортні шляхи, складські приміщення, зрошувальні системи, енергетичні мережі, телекомунікації та інші, які забезпечують функціонування та розвиток сільського господарства.

Розвиток інфраструктури є надважливим чинником ефективності діяльності суб'єктів господарювання аграрного сектору економіки, адже:

- розвинена мережа автомобільних та залізничних доріг, портів та аеропортів забезпечує швидке та ефективне транспортування сільськогосподарської продукції від місця виробництва до споживача,;

- якісні дороги та сучасні транспортні засоби дозволяють зменшити транспортні витрати, що підвищує конкурентоспроможність сільськогосподарської продукції;

- розвинена транспортна інфраструктура сприяє розширенню доступу сільськогосподарських виробників до ринків збуту, зокрема, до віддалених регіонів та за кордон;

- сучасні складські приміщення, обладнані системами охолодження та вентиляції, дозволяють зберігати сільськогосподарську продукцію протягом тривалого часу, зберігаючи її якість та запобігаючи втратам;

- розвинена складська інфраструктура дозволяє регулювати поставки сільськогосподарської продукції на ринок, запобігаючи її надлишку або дефіциту, що сприяє стабілізації цін;

- зрошувальні системи забезпечують регулярне зрошення сільськогосподарських культур, що сприяє підвищенню врожайності та збільшенню виробництва сільськогосподарської продукції;

- зрошення дозволяє зменшити залежність сільського господарства від погодних умов, забезпечуючи стабільність виробництва та зменшуючи ризики втрати врожаю через посуху;

- надійне та доступне енергопостачання є необхідним для функціонування суб'єктів господарювання, зокрема, для роботи обладнання, освітлення, опалення тощо;

- розвиток енергетичної інфраструктури сприяє впровадженню сучасних енергозберігаючих технологій у сільському господарстві;

- сучасні телекомунікаційні системи забезпечують доступ сільськогосподарських виробників до інформації про ринки, ціни, нові технології, що сприяє прийняттю обґрунтованих управлінських рішень.

Інтернет та інші телекомунікаційні засоби дозволяють упроваджувати digital-маркетинг (Дяченко, 2024), адже охоплює широкий спектр технологій та інструментів, які можуть бути застосовані на різних етапах інвестиційного

циклу – від пошуку проєктів до моніторингу їх реалізації та оцінки результатів.

- розвивати електронну торгівлю сільськогосподарською продукцією, розширюючи ринки збуту та зменшуючи витрати на маркетинг.

Розвиток інфраструктури аграрного сектору в Україні стикається з низкою викликів, серед яких:

- недостатнє фінансування - модернізація та розвиток інфраструктури потребують значних інвестицій, які часто є недоступними для суб'єктів господарювання;

- застарілість інфраструктури - значна частина інфраструктури аграрного сектору є застарілою та потребує модернізації;

- бюрократичні перешкоди - складні процедури отримання дозволів та погоджень можуть затримувати реалізацію інфраструктурних проєктів.

Проте, розвиток інфраструктури аграрного сектору має великі перспективи. Уряд України розробляє та реалізує ряд програм, спрямованих на залучення інвестицій у розвиток інфраструктури, зокрема, за рахунок міжнародних фінансових інституцій. Важливим напрямом є також розвиток державно-приватного партнерства у сфері інфраструктурних проєктів.

Розвиток сучасної та ефективної інфраструктури є ключовим чинником забезпечення ефективності регулювання інноваційного розвитку аграрного сектору економіки України. Інвестиції в інфраструктуру сприяють підвищенню ефективності сільськогосподарського виробництва, зменшенню витрат, розширенню доступу до ринків збуту та залученню інновацій. Для досягнення успіху у цій сфері необхідно подолати існуючі виклики та створити сприятливі умови для залучення інвестицій та реалізації інфраструктурних проєктів. Будівництво та реконструкція доріг, розвиток транспортної інфраструктури дозволяє забезпечити своєчасну доставку сільськогосподарської продукції на ринки збуту та зменшити транспортні витрати.

Ефективним чинником забезпечення ефективності регулювання інноваційного розвитку аграрного сектору економіки України є відновлення та розвиток зрошувальних систем.

Зрошувальні системи відіграють вирішальну роль у забезпеченні сталого розвитку та підвищенні ефективності регулювання інноваційного розвитку аграрного сектору економіки України. Вони є запорукою отримання стабільних та високих врожаїв, особливо в умовах зміни клімату та збільшення кількості засух, адже:

- зрошення дозволяє забезпечити рослини необхідною кількістю вологи, що сприяє їх росту та розвитку, а отже, й підвищенню врожайності сільськогосподарських культур;

- зрошувані землі менш залежні від погодних умов, що забезпечує стабільність виробництва та зменшує ризики втрати врожаю через засуху;

- зрошення дозволяє вирощувати вологолюбні культури, які в умовах недостатнього зволоження не можуть рости;

- забезпечення рослин достатньою кількістю вологи сприяє покращенню якості сільськогосподарської продукції;

- зрошення дозволяє більш ефективно використовувати земельні ресурси, отримуючи більші врожаї з меншої площі.

На жаль, зрошувальні системи в Україні знаходяться у занедбаному стані.

Більшість з них потребують відновлення та модернізації. Це пов'язано з різними чинниками, такими як:

- недостатнє фінансування, адже протягом багатьох років зрошувальні системи не отримували достатнього фінансування для підтримки їх у належному стані;
- застарілі технології є неефективними та потребують заміни;
- відсутність належного управління зрошувальними системами призводить до їх зношення та виходу з ладу (*Спринчук, 2024*).

Відновлення та розвиток зрошувальних систем є важливим завданням для аграрного сектору України. Для цього необхідно:

- залучити значні інвестиції для відновлення та модернізації зрошувальних систем.
- упроваджувати сучасні технології зрошення, які є ефективними та екологічно безпечними;
- забезпечити належне управління зрошувальними системами, включаючи їх технічне обслуговування та ремонт;
- підготувати кваліфіковані кадри для роботи зі зрошувальними системами;
- забезпечити державну підтримку повинна відігравати активну роль у відновленні та розвитку зрошувальних систем, надаючи фінансову підтримку, створюючи сприятливі умови для залучення інвестицій та сприяючи впровадженню сучасних технологій.

Відновлення та розвиток зрошувальних систем є важливим чинником забезпечення ефективності регулювання інноваційного розвитку аграрного сектору економіки України. Це дозволить підвищити врожайність, забезпечити стабільність виробництва, розширити можливості для вирощування різних культур та покращити якість сільськогосподарської продукції.

Ефективним чинником забезпечення ефективності регулювання інноваційного розвитку аграрного сектору України є меліорація земель, як комплекс заходів, спрямованих на поліпшення ґрунтів, їх фізичних, хімічних та біологічних властивостей.

Меліорація відіграє важливу роль у підвищенні продуктивності сільськогосподарських угідь та забезпеченні сталого розвитку аграрного сектору, адже:

- меліоративні заходи, такі як будівництво та відновлення зрошувальних систем, дозволяють збільшити площу зрошуваних земель, що особливо важливо в умовах посушливого клімату південних регіонів України;
- меліоративні заходи, такі як створення захисних лісосмуг, терасування схилів та інші, запобігають ерозії ґрунтів, зберігаючи їх родючість;
- меліорація дозволяє регулювати водний режим ґрунтів, запобігаючи їх перезволоженню або пересиханню, що створює оптимальні умови для росту рослин.

Виокремлюють декілька видів меліоративних робіт (табл. 4).

Меліоративні системи в Україні знаходяться у занедбаному стані.

Більшість з них потребують відновлення та модернізації. Це пов'язано з різними чинниками, такими як:

- протягом багатьох років меліоративні системи не отримували

достатнього фінансування для підтримки їх у належному стані;

- більшість меліоративних систем використовують застарілі технології, які є неефективними та потребують заміни;

- управління меліоративними системами часто є неефективним, що призводить до їх зношення та виходу з ладу.

Таблиця 4. Види меліоративних заходів

№ з/п	Напрямок	Характеристика
1.	Гідротехнічна меліорація	будівництво та відновлення зрошувальних та осушувальних систем, каналів, дамб, водосховищ тощо
2.	Агротехнічна меліорація	обробку ґрунту, внесення добрив, посів сидеральних культур та інші заходи, спрямовані на поліпшення родючості ґрунтів
3.	Лісомеліорація	створення захисних лісосмуг, терасування схилів та інші заходи, спрямовані на запобігання ерозії ґрунтів
4.	Хімічна меліорація	внесення в ґрунт речовин, які поліпшують його хімічні властивості, наприклад, вапнування кислих ґрунтів

Відновлення та розвиток меліоративних систем є важливим завданням для аграрного сектору України. Для цього необхідно:

- залучити значні інвестиції для відновлення та модернізації меліоративних систем;

- упроваджувати сучасні технології зрошення та меліорації, які є ефективними та екологічно безпечними;

- забезпечити належне управління меліоративними системами, включаючи їх технічне обслуговування та ремонт;

- підготувати кваліфіковані кадри для роботи з меліоративними системами;

- забезпечити дієву державну підтримку відновленню та розвитку меліоративних систем, яка б передбачала фінансову підтримку, створення сприятливих умов для залучення інвестицій та сприяла впровадженню сучасних технологій.

Відновлення та розвиток зрошувальних систем, проведення меліоративних заходів дозволяє збільшити площі зрошуваних земель та підвищити врожайність.

Меліорація земель є важливим чинником забезпечення ефективності регулювання інноваційного розвитку аграрного сектору економіки України. Вона дозволяє збільшити площу зрошуваних земель, підвищити врожайність, розширити можливості для вирощування різних культур та покращити якість сільськогосподарської продукції.

Ефективним механізмом забезпечення ефективності регулювання інноваційного розвитку аграрної сфери економіки України є створення сучасних логістичних центрів для зберігання, переробки та упаковки сільськогосподарської продукції.

Розвиток сучасної логістичної інфраструктури є ключовим чинником підвищення ефективності регулювання інноваційного розвитку аграрного сектору економіки України. Створення сучасних логістичних центрів для зберігання, переробки та упаковки сільськогосподарської продукції відіграє вирішальну роль у

забезпеченні якості, зменшенні втрат та ефективному збуті продукції як на ендегенному, так і на екзогенному ринках, адже:

- сучасні логістичні центри, обладнані системами контролю температури та вологості, дозволяють зберігати сільськогосподарську продукцію протягом тривалого часу, запобігаючи її псуванню та зменшуючи втрати;
- забезпечення належних умов зберігання дозволяє зберегти якість сільськогосподарської продукції, її смакові властивості та поживну цінність;
- логістичні центри можуть включати в себе потужності для переробки сільськогосподарської продукції, що дозволяє створювати продукти з доданою вартістю, розширювати асортимент та задовольняти потреби різних категорій споживачів;
- логістичні центри можуть бути обладнані сучасними лініями для пакування сільськогосподарської продукції відповідно до вимог ринку, сучасна упаковка відіграє важливу роль у збереженні якості продукції, її привабливості для споживачів та зручності транспортування.

Сучасні логістичні центри використовують передові технології управління, що дозволяє оптимізувати процеси зберігання, переробки, пакування та транспортування продукції, зменшуючи витрати та забезпечуючи своєчасну доставку.

Наявність сучасної логістичної інфраструктури сприяє розширенню ринків збуту сільськогосподарської продукції, включаючи експорт.

Створення сучасних логістичних центрів підвищує конкурентоспроможність аграрного сектору України, дозволяючи виробникам пропонувати якісну продукцію за конкурентними цінами.

Сучасні логістичні центри повинні:

- забезпечувати повний цикл логістичних операцій, від зберігання та переробки до пакування та транспортування;
- використовувати сучасні технології, такі як системи управління запасами, автоматизовані системи зберігання та обробки даних, що дозволяє підвищити ефективність роботи центрів;
- відповідати міжнародним стандартам якості та безпеки харчової продукції;
- дотримуватись принципу енергоефективності шляхом використання енергозберігаючих технологій та відновлюваних джерел енергії, що сприятиме зменшенню витрат на утримання центрів;
- бути розташовані поблизу транспортних магістралей та мати зручний доступ для виробників та споживачів.

З метою розширення мережі сучасних логістичних центрів необхідно залучити інвестиції для будівництва нових та модернізації чи переобладнання наявних.

Створення сучасної та ефективної мережі логістичних центрів є ключовим чинником підвищення ефективності регулювання інноваційного розвитку аграрного сектору економіки України. Залучення інвестицій відіграє вирішальну роль у реалізації цього амбітного завдання.

З метою залучення інвестицій для створення мережі сучасних логістичних центрів необхідно здійснити ідентифікацію потреби аграрного сектору в логістичних послугах, у ході якої:

- провести комплексний аналіз існуючої інфраструктури, обсягів

виробництва сільськогосподарської продукції, потреб у зберіганні, переробці та транспортуванні;

- на основі цього комплексного аналізу розробити детальну концепцію створення мережі логістичних центрів, яка включає в себе:

- ✓ визначення оптимального розташування центрів: враховуючи логістичні потоки, транспортну інфраструктуру та потреби регіонів;

- ✓ визначення функціональності центрів: які послуги вони будуть надавати (зберігання, переробка, пакування, транспортування тощо);

- ✓ розрахунок необхідних інвестицій для будівництва, обладнання та функціонування центрів;

- ✓ розробку бізнес-плану з обґрунтуванням економічної доцільності проєкту та прогнозом окупності інвестицій;

- ✓ пошук потенційних інвесторів.

Залучення інвестицій потребує активного пошуку потенційних інвесторів, як ендегенних, так і екзогенних. Серед них можуть бути:

- агрохолдинги та великі сільськогосподарські виробники, які зацікавлені у створенні власної логістичної інфраструктури для забезпечення ефективного збуту своєї продукції;

- транспортно-логістичні компанії, адже вони зацікавлені у розширенні своєї діяльності та створенні нових логістичних центрів;

- інвестиційні фонди зацікавлені у довгострокових інвестиціях у перспективні проєкти;

- банки можуть надавати кредити для реалізації проєктів зі створення логістичних центрів.

- міжнародні організації можуть надавати гранти чи кредити на пільгових умовах для розвитку аграрного сектору.

Для успішного залучення інвестицій необхідно презентувати інвестиційний проєкт потенційним інвесторам. Презентація повинна містити:

- детальну інформацію про проєкт: концепцію, функціональність, розташування, обсяг необхідних інвестицій;

- обґрунтування економічної доцільності: прогнози щодо обсягів виробництва, цін, доходів та окупності інвестицій;

- інформацію про конкурентні переваги: чому саме цей проєкт є привабливим для інвесторів;

- гарантії повернення інвестицій: які механізми будуть використані для забезпечення повернення інвестицій.

Залучення інвестицій потребує створення сприятливого інвестиційного клімату в країні. Це включає в себе:

- чітке та прозоре законодавство, яке регулює інвестиційну діяльність;

- гарантування захисту прав інвесторів та їх інвестицій;

- зменшення адміністративного тиску на бізнес та спрощення процедур отримання дозволів та ліцензій;

- надання податкових пільг для інвесторів, які вкладають кошти в розвиток аграрного сектору;

- створення сучасної транспортної, енергетичної та телекомунікаційної

інфраструктури;

- державну підтримку у залученні інвестицій для створення мережі логістичних центрів.

Серед механізмів державної підтримки у залученні інвестицій для створення мережі логістичних центрів варто виокремити розробку та реалізацію державних програм, спрямованих на розвиток логістичної інфраструктури аграрного сектору.

Розвиток логістичної інфраструктури є критично важливим для забезпечення ефективності регулювання інноваційного розвитку аграрного сектору України. Ефективна логістика дозволяє зменшити втрати продукції, зберегти її якість, розширити ринки збуту та підвищити ефективність виробництва.

Державні програми відіграють ключову роль у створенні сприятливих умов для розвитку логістичної інфраструктури, залучення інвестицій та координації зусиль різних учасників ринку.

Державні програми, спрямовані на розвиток логістичної інфраструктури аграрного сектору України, повинні мати чітко визначені цілі та завдання, серед яких можуть бути:

- створення сучасної та ефективної мережі логістичних центрів: будівництво нових та модернізація існуючих складських приміщень, обладнаних сучасними системами зберігання та управління;

- розвиток транспортної інфраструктури: будівництво та реконструкція доріг, залізниць, портів та аеропортів, що забезпечують ефективне транспортування сільськогосподарської продукції;

- упровадження сучасних технологій: сприяння впровадженню сучасних інформаційних технологій, систем управління логістикою, що дозволяють оптимізувати процеси та зменшити витрати;

- залучення інвестицій: створення сприятливих умов для залучення інвестицій у розвиток логістичної інфраструктури, зокрема, за рахунок надання податкових пільг, гарантій та інших видів підтримки;

- підтримка малого та середнього бізнесу: створення умов для участі малого та середнього бізнесу у розвитку логістичної інфраструктури, зокрема, шляхом надання грантів, субсидій та інших видів підтримки;

- підготовка кадрів: забезпечення підготовки кваліфікованих кадрів для роботи в сучасних логістичних центрах (Василина О., 2024).

В Україні вже реалізуються деякі державні програми, спрямовані на розвиток логістичної інфраструктури аграрного сектору, зокрема:

- Програма розвитку аграрного сектору економіки на період до 2020 року.

- Стратегія розвитку сільського господарства та сільських територій на період до 2030 року.

Проте, необхідно продовжувати роботу над їх удосконаленням та розробкою нових програм, враховуючи сучасні виклики та потреби аграрного сектору.

Для досягнення поставлених цілей та завдань державні програми повинні передбачати ефективні заходи щодо її реалізації (табл. 5).

Розробка та реалізація ефективних державних програм, спрямованих на розвиток логістичної інфраструктури аграрного сектору, є важливим чинником підвищення ефективності регулювання інноваційного розвитку української

сільськогосподарської продукції на ендегенному та екзогенному ринках. Державні програми повинні передбачати чіткі цілі та завдання, ефективні механізми реалізації, достатнє фінансування та координацію діяльності різних учасників ринку.

Державно-приватне партнерство є важливим інструментом для забезпечення ефективності регулювання інноваційного розвитку аграрного сектору економіки України. Воно передбачає співпрацю між державою та приватним сектором з метою реалізації спільних проєктів, спрямованих на розвиток аграрного сектору та підвищення його ефективності.

Таблиця 5. Заходи реалізації державних програм, спрямованих на розвиток логістичної інфраструктури аграрного сектору України

№ з/п	Заходи	Характеристика
1.	Розробка та затвердження стратегій та планів	Визначення пріоритетних напрямів розвитку логістичної інфраструктури, розробка конкретних планів дій та заходів
2.	Фінансове забезпечення	Виділення необхідних коштів з державного бюджету, залучення коштів міжнародних фінансових організацій та приватних інвесторів
3.	Нормативно-правове регулювання	Створення сприятливого правового поля для розвитку логістичної інфраструктури, спрощення процедур отримання дозволів та ліцензій
4.	Координація діяльності	Забезпечення координації діяльності різних органів влади, підприємств та організацій, задіяних у розвитку логістичної інфраструктури
5.	Моніторинг та оцінка	Здійснення моніторингу та оцінки ефективності реалізації програм, внесення необхідних змін та корегувань

Серед форм державно-приватного партнерства в аграрному секторі доцільно виокремити:

- договори концесії, при яких держава передає приватному сектору право на будівництво та експлуатацію об'єктів інфраструктури, таких як дороги, елеватори тощо;
- створення спільних підприємств для реалізації конкретного проєкту;
- договори про співпрацю для реалізації спільних проєктів.
- інвестиційні проєкти, у ході впровадження яких держава та приватний сектор інвестують кошти в спільні проєкти.

Ефективним чинником забезпечення ефективності регулювання інноваційного розвитку аграрного сектору економіки України є створення сприятливих умов для інвесторів.

Забезпечення ефективності регулювання інноваційного розвитку аграрного сектору економіки України є стратегічно важливим завданням для держави. Одним із ключових чинників досягнення цієї мети є створення сприятливих умов для залучення інвестицій, адже саме інвестиції є каталізатором розвитку та модернізації аграрного сектору економіки України (табл. 6):

Таблиця 6. Вплив інвестицій на конкурентоспроможність аграрного сектору економіки України

Напрямок	Характеристика
Модернізація виробництва	Залучення інвестицій дозволяє оновлювати матеріально-технічну базу суб'єктів господарювання, впроваджувати сучасні технології та обладнання, що сприяє підвищенню продуктивності та ефективності виробництва
Розвиток інфраструктури	Інвестиції спрямовуються на розвиток логістичної інфраструктури, будівництво складських приміщень, доріг, зрошувальних систем, що забезпечує якісне зберігання та транспортування сільськогосподарської продукції
Упровадження інновацій	Інвестиції сприяють залученню інновацій, розробці та впровадженню нових сортів рослин, порід тварин, технологій обробки ґрунту, що підвищує конкурентоспроможність продукції, а відтак, й конкурентоспроможність аграрного сектору економіки України
Створення нових робочих місць	Залучення інвестицій сприяє створенню нових робочих місць у сільській місцевості, що зменшує безробіття та сприяє розвитку регіонів
Збільшення експортного потенціалу	Інвестиції в аграрний сектор дозволяють збільшити обсяги виробництва якісної сільськогосподарської продукції, що користується попитом на світових ринках, та розширити експортний потенціал країни

Необхідність залучення інвестицій у аграрний сектор економіки України обумовлює потребу сприятливих умов для інвесторів, серед яких (табл. 7):

Таблиця 7. Передумови сприятливого інвестиційного клімату

№ з/п	Напрямок	Характеристика
1.	Стабільне законодавство	Інвестори потребують чіткого та стабільного законодавства, яке регулює інвестиційну діяльність та захищає їх права
2.	Прозора та зрозуміла система оподаткування	Податкова система повинна бути прозорою та зрозумілою для інвесторів, а податкові ставки конкурентними
3.	Мінімізація адміністративних бар'єрів	Процедури отримання дозволів та ліцензій повинні бути максимально спрощеними та швидкими
4.	Доступ до фінансових ресурсів	Інвестори повинні мати доступ до фінансових ресурсів, зокрема, кредитів на вигідних умовах
5.	Розвинена інфраструктура	Наявність розвинутої транспортної, логістичної та енергетичної інфраструктури є важливим чинником для інвесторів
6.	Кваліфікована робоча сила	Наявність кваліфікованої робочої сили є важливим чинником для успішної реалізації інвестиційних проєктів

7.	Захист прав власності	Інвестори повинні бути впевнені у захисті своїх прав власності на землю та інші активи
8.	Боротьба з корупцією	Корупція є серйозною перешкодою для залучення інвестицій, тому боротьба з нею є важливим завданням для держави

З метою формування сприятливого інвестиційного клімату в аграрному секторі економіки України необхідно здійснити удосконалення законодавства, спрощення адміністративних процедур, створення сприятливого податкового клімату (*Драган, 2024*), розвиток інфраструктури, підтримка освіти та науки, боротьба з корупцією (табл. 8):

Таблиця 8. Заходи щодо формування сприятливого інвестиційного клімату в аграрному секторі економіки України

№ з/п	Напрямок	Характеристика
1.	Удосконалення законодавства	Необхідно ухвалити чітке та стабільне законодавство, яке регулює інвестиційну діяльність та захищає права інвесторів
2.	Спрощення адміністративних процедур	Необхідно максимально спростити процедури отримання дозволів та ліцензій, зменшити кількість бюрократичних бар'єрів
3.	Створення сприятливого податкового клімату	Необхідно знизити податкові ставки та запровадити податкові пільги для інвесторів, які вкладають кошти в розвиток аграрного сектору
4.	Розвиток інфраструктури	Необхідно інвестувати в розвиток транспортної, логістичної та енергетичної інфраструктури, що є важливим чинником для інвесторів
5.	Підтримка освіти та науки	Необхідно створювати умови для підготовки кваліфікованих кадрів для роботи в аграрному секторі, сприяти розвитку наукових досліджень та інновацій
6.	Участь у фінансуванні проєктів	Надання грантів, субсидій чи кредитів на пільгових умовах.
7.	Інформаційна підтримка	Надання інвесторам інформації про інвестиційні можливості в аграрному секторі
8.	Боротьба з корупцією	Необхідно посилити боротьбу з корупцією, забезпечити прозорість та підзвітність діяльності органів влади

Створення сприятливих умов для інвесторів є ключовим чинником забезпечення конкурентоспроможності аграрного сектору економіки України.

Залучення інвестицій дозволить модернізувати виробництво, розвинути інфраструктуру, залучити інновації та підвищити ефективність сільськогосподарського виробництва.

Для досягнення цієї мети необхідно удосконалити законодавство, спростити

адміністративні процедури, створити сприятливий податковий клімат, розвинути інфраструктуру, підтримати освіту та науку, посилити боротьбу з корупцією, передбачити надання податкових пільг для інвесторів, спрощення процедур та гарантування захисту інвестицій.

Висновки. Аграрний сектор економіки України має значний потенціал для розвитку та забезпечення конкурентоспроможності на світовому ринку. Проте, для досягнення цієї мети необхідно активно впроваджувати інноваційні механізми, які дозволять підвищити ефективність виробництва, якість продукції та зменшити витрати.

Основними напрями інноваційного розвитку аграрного сектору є:

- цифровізація шляхом впровадження точного землеробства: використання дронів, супутників, сенсорів та інших технологій для збору даних про стан ґрунту, посівів та погодних умов, що дозволяє оптимізувати внесення добрив, полив та інші агротехнічні заходи, які підвищує врожайність та зменшує витрати;

- автоматизація виробництва шляхом використання роботів, автоматизованих систем управління та інших технологій, які сприяють зменшенню залежності від людського фактору, підвищенню продуктивності та зниженню собівартості продукції;

- створення електронних платформ для торгівлі та використання механізмів публічного digital-маркетингу формують додаткові можливості виробникам знаходити нових покупців, зменшуючи витрати на збут та, як наслідок, нівелюють потребу підвищення ціни на продукцію;

- впровадження штучного інтелекту є ключовим чинником підвищення конкурентоспроможності аграрного сектору України, адже застосування штучного інтелекту в аграрній сфері може допомогти вирішити багато проблем, з якими стикається галузь, та відкрити нові можливості для розвитку;

- розвиток біотехнологій, який сприяє створенню сортів рослин з високою врожайністю, стійкістю до хвороб та шкідників, а також породи тварин з високою продуктивністю та якістю м'яса;

- виробництво біопрепаратів для захисту рослин та тварин дозволяє зменшити використання хімічних речовин, що є більш безпечним для довкілля та здоров'я людини;

- удосконалення системи управління якістю та безпечністю продукції шляхом впровадження міжнародних стандартів – сертифікація сільськогосподарської продукції відповідно до міжнародних стандартів якості та безпеки дозволяє підвищити її конкурентоспроможність на світовому ринку;

- створення систем контролю якості на всіх етапах виробництва обумовлює можливість відстеження якості продукції від поля до прилавка, що формує засади суспільної довіри до аграрного сектора;

- розвиток інфраструктури – модернізація транспортної інфраструктури, елеваторів та інших об'єктів інфраструктури дозволяє зменшити витрати на транспортування та зберігання сільськогосподарської продукції; розвиток сучасних логістичних центрів дозволяє оптимізувати поставки сільськогосподарської продукції та зменшити час її доставки до споживачів;

- створення сприятливого інвестиційного клімату сприятиме залученню

інвестицій у аграрний сектор економіки;

– розвиток державно-приватного партнерства сприятиме залученню приватних інвестицій до реалізації інфраструктурних проєктів та інших програм розвитку аграрного сектору, збільшенню обсягів фінансування та прискоренню їх реалізації.

Успішне впровадження інноваційних механізмів в аграрному секторі економіки України є запорукою його сталого розвитку та забезпечення конкурентоспроможності на світовому ринку. Для досягнення цієї мети необхідно об'єднати зусилля держави, бізнесу та наукових установ, створити сприятливі умови для інноваційного розвитку та забезпечити ефективне використання ресурсів.

References:

- Василина О., Попадинець Н., Яхно Т., Садура О., Кравчик Ю. (2024). Розвиток аграрної сфери: трансформація логістичних зв'язків та економічна ефективність підприємств зернової продукції. *Herald of Khmelnytskyi National University. Economic Sciences*, 328(2), 477-482. <https://doi.org/10.31891/2307-5740-2024-328-71>
- Демченко О. Механізм впливу сільськогосподарської кооперації на розвиток людського капіталу сільських територій України. *Український журнал прикладної економіки та техніки*. 2024. Том 9. № 1. С. 327-331. <https://doi.org/10.36887/2415-8453-2024-1-55>
- Драган І., Даций Н., Антонова Л. Регулювання виробництва в аграрному секторі України із застосуванням механізмів бюджетного та позабюджетного інвестування. *Інвестиції: практика та досвід*. 2024. № 1. С. 95-102. <https://doi.org/10.32702/2306.6814.2024.1.95>
- Дяченко В. С., Дяченко Н. П. 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](https://doi.org/10.52058/2708-7530-2024-2(44)-245-254)
- Карбовська Л., Мазур Ю., Железняк К., Козлова А., Мельник Б., Скрипцов С. Формування системи управління відходами в аграрному секторі економіки України: організаційний та фінансовий аспекти. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2024. Том 5(58). С. 367-379. <https://doi.org/10.55643/fcaptp.5.58.2024.4462>
- Левченко І., Шарий Г., Андріяш А. Ринок органічної продукції України та його привабливість для залучення іноземних інвестицій. *Агросвіт*. 2023. № 15. С. 43-51. <https://doi.org/10.32702/2306-6792.2023.15.43>
- Сичук О. В. (2024). Діагностика розвитку ринку органічної продукції в Україні. *Проблеми сучасних трансформацій. Серія: економіка та управління*, (15). <https://doi.org/10.54929/2786-5738-2024-15-03-02>
- Спринчук Н. Економічна ефективність інвестицій в зрощувальні технології. *Агросвіт*. 2024. № 15. С. 70-74. <https://doi.org/https://orcid.org/0000L0002L3118L2009>
- Юрчук Н., Кіпоренко С. Цифровізація сільського господарства: виклики і можливості для фермерських господарств. *Агросвіт*. 2024. № 19. С. 53-62. <https://doi.org/10.32702/2306-6792.2024.19.53>

References:

- Vasylyna O., Popadynets N., Yakhno T., Sadura O., Kravchik Yu. (2024). Development of the agricultural sector: transformation of logistics connections and economic efficiency of grain production enterprises. *Herald of Khmelnytskyi National University. Economic Sciences*. <https://doi.org/10.31891/2307-5740-2024-328-71>
- Demchenko O. (2024). The mechanism of the influence of agricultural cooperation on the development of human capital in rural areas of Ukraine. *Ukrainskyi zhurnal prykladnoi ekonomiky ta tekhniky*. <https://doi.org/10.36887/2415-8453-2024-1-55>.
- Drahan I., Datsii N., Antonova L. (2024). Regulation of production in the agricultural sector of Ukraine using budgetary and extra-budgetary investment mechanisms. *Investytsii: praktyka ta dosvid*.

<https://doi.org/10.32702/2306-6814.2024.1.95>

- Diachenko V. S., Diachenko N. P. (2024). Публічний digital-маркетинг як елемент державної інформаційної політики. *Naukovi perspektyvy*. [https://doi.org/10.52058/2708-7530-2024-2\(44\)-245-254](https://doi.org/10.52058/2708-7530-2024-2(44)-245-254)
- Karbovska L., Mazur Yu., Zhelezniak K., Kozlova A., Melnyk B., Skryptsov S. (2024). Formation of a waste management system in the agricultural sector of the Ukrainian economy: organizational and financial aspects. *Finansovo-kredytna diialnist: problemy teorii ta praktyky*. <https://doi.org/10.55643/fcaptp.5.58.2024.4462>
- Levchenko I., Sharyi H., Andriiash A. (2023). The Ukrainian organic market and its attractiveness for attracting foreign investment. *Ahrosvit*. <https://doi.org/10.32702/2306-6792.2023.15.43>
- Sychuk O. (2024). Diagnostics of the development of the organic products market in Ukraine. *Problemy suchasnykh transformatsii*. <https://doi.org/10.54929/2786-5738-2024-15-03-02>
- Sprynchuk N. (2024). Economic efficiency of investments in irrigation technologies. *Ahrosvit*. <https://doi.org/https://orcid.org/0000L0002L3118L2009>
- Iurchuk N., Kiporenko S. (2024). Digitalization of agriculture: challenges and opportunities for farms. *Ahrosvit*. <https://doi.org/10.32702/2306-6792.2024.19.53>

CHAPTER 9. COMPLIANCE CONTROL AS A TOOL FOR ENSURING ECONOMIC SECURITY IN THE CORPORATE GOVERNANCE SYSTEM

Svitlana FIMYAR

Candidate of Economics, Associate Professor of the Department of Economics, Finance,
Accounting, Mathematical and Information Disciplines
Cherkasy Branch of the Ukrainian Higher Education Establishment European University
(83, Smilyanska str., Cherkasy, 18008, Ukraine)

fimyar@ukr.net

<https://orcid.org/0000-0003-0432-2587>

Abstract. The research problem is the formation of a compliance system as a tool for ensuring economic security, taking into account the influence of specific organizational and legal factors of corporate governance. The content of economic security and its role in corporate governance are defined. It has been proven that the priority task of ensuring the economic security of corporate entities in the modern world is to create the prerequisites for their stable and effective activities, dynamic growth, and the formation of the potential for sustainable development of corporate structures in the future.

The types and tools of compliance to ensure the economic security of corporations are investigated. The conducted research allowed us to formulate a definition of compliance as a set of legislative, professional and ethical norms and rules, both general in nature and formed by each corporation individually, but mandatory for all employees of private, state and public structures, regardless of their position. A general conclusion was made that the formation of the corporation's compliance system directly depends on its organizational and legal form, and the company's publicity or non-publicity is one of the main factors that determine the need for the creation and effective functioning of compliance in its organizational structure.

Keywords: economic security, compliance system, compliance control, corporate governance, public and private organizational forms of corporations.

КОМПЛІАЄНС-КОНТРОЛЬ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ В СИСТЕМІ КОРПОРАТИВНОГО УПРАВЛІННЯ

Анотація. Проблематикою дослідження є формування системи комплаєнсу як інструменту забезпечення економічної безпеки з урахуванням впливу конкретних організаційно-правових факторів корпоративного управління. Визначено зміст економічної безпеки та її роль у корпоративному управлінні. Доведено, що пріоритетним завданням забезпечення економічної безпеки корпоративних утворень в сучасному світі є створення передумов для стабільної та ефективної їх діяльності, динамічного зростання, формування потенціалу сталого розвитку корпоративних структур в перспективі.

Досліджено види та інструменти комплаєнсу для забезпечення економічної безпеки корпорацій. Проведені дослідження дозволили сформулювати визначення комплаєнсу як зведення законодавчих, професійних та етичних норм і правил, як загального характеру, так

і сформованих кожною корпорацією індивідуально, але при цьому обов'язкових для дотримання всіма працівниками приватних, державних та громадських структур незалежно від їх положення. Зроблено загальний висновок про те, що формування комплаєнс-системи корпорації безпосередньо залежить від її організаційно-правової форми, а публічність або непублічність компанії є одним із основних факторів, що визначають необхідність створення та ефективного функціонування комплаєнсу в її організаційній структурі.

Ключові слова: економічна безпека, комплаєнс-система, комплаєнс-контроль, корпоративне управління, публічна та приватна організаційні форми корпорацій.

Вступ. Значна частина науково-практичних розробок, що здійснюються в даний час, спрямована на забезпечення максимально безпечного функціонування бізнесу, збереження інформації, її обмежену доступність. Однак будь-який навіть найнадійніший захист, так само як і детально опрацьоване правове регулювання в кінцевому рахунку нівелюється людським фактором. Слід зазначити, що основна частина проблем, пов'язаних із порушенням встановлених законами та внутрішніми документами правил, є результатом навмисних або необережних дій співробітників компанії. Для запобігання їх у будь-якій організації необхідна проста, на інтуїтивному рівні зрозуміла і водночас глибоко продумана система. Сьогодні такою системою, на нашу думку, є комплаєнс.

Актуальність комплаєнсу безумовно визнана міжнародною практикою і усвідомлюється дедалі більшою кількістю вітчизняних керівників корпоративного бізнесу. В сучасних умовах комплаєнс є одним з найважливіших напрямів превентивного реагування на ризики, що виникають у внутрішньому бізнес-середовищі, а також умови, що генеруються на національному та міжнародному законодавчому рівні. Змінюються технології, уточнюються принципи ведення бізнесу, удосконалюється законодавство, виникають непередбачені обставини (санкції). Все це призводить до значної та досить оперативної зміни нормативно-регулятивної обстановки, що збільшує цінність комплаєнс-функції.

Одним із функціональних завдань комплаєнсу є впровадження в корпорацію внутрішніх правил, що регулюють поведінку та діяльність співробітників у частині взаємодії з клієнтами та контрагентами, інформаційного обміну між внутрішніми структурними підрозділами, ефективної роботи з державними та громадськими організаціями. Комплаєнс у більш вузькому значенні – це, перш за все, відповідність внутрішніх параметрів та документів організації вимогам чинного законодавства.

У вітчизняному законодавстві відсутнє офіційне визначення комплаєнсу, у зв'язку з чим у науковій літературі ще не склалося її єдиного підходу до тематики, проте на практиці комплаєнс – вже невід'ємний елемент регулювання та корпоративного управління.

Функціонал комплаєнсу, що реалізується, як правило, юридичним підрозділом, тісно пов'язаний з усіма напрямками діяльності будь-якої компанії, а отже, і з усіма її структурними підрозділами: операційним, комерційними та некомерційними закупівлями, внутрішнім контролем, фінансовим моніторингом, службою безпеки, аудиту та операційних ризиків, персоналу та т.ін. Будучи важливою ланкою системи корпоративного управління, комплаєнс сьогодні формує відповідну потребу у конкретних спеціалістах, що визначає необхідність відповідних досліджень.

Таким чином, в даний час комплаєнс на практиці стає все більш затребуваною функцією менеджменту і фактично виділяється в окремий науковий напрям, що вимагає чіткої оцінки даного явища та глибокого наукового опрацювання піднятої тематики.

Метою дослідження є конкретизація теоретичних та практичних аспектів комплаєнс-контролю як інструменту забезпечення економічної безпеки в системі корпоративного управління. Для досягнення мети поставлені наступні завдання:

- визначити зміст економічної безпеки та її роль у корпоративному управлінні;
- дослідити види та інструменти комплаєнсу для забезпечення економічної безпеки корпорацій.

Формування системи комплаєнсу як інструменту забезпечення економічної безпеки з урахуванням впливу конкретних організаційно-правових факторів корпоративного управління (форми власності, організаційно-правової форми та ін.) є предметом даного дослідження.

1. Зміст економічної безпеки та її роль у корпоративному управлінні

Поняття економічної безпеки є достатньо новим в теорії управління, але широко використовуваним в практичній діяльності корпоративних структур західних країн. Безпека, на думку більшості вчених, означає ситуацію відсутності небезпеки. Така позиція є наслідком того, що в економічних словниках в якості безпеки розглядається стан, за якого не загрожує небезпека (як загроза, згідно з цими ж словниками).

Більш детально розглядають поняття «небезпека» ряд авторів (*Польова, Когут, Дума, 2024*), які розуміють її як існуючу або потенційну можливість дії загрози, вплив якої може завдати шкоди будь-якому суб'єкту або об'єкту; об'єктивно існуючу реальність, яка може порушити стан рівноваги суб'єктів та призвести до негативних наслідків; усвідомлену, але не фатальну ймовірність заподіяння шкоди, яка визначається наявністю об'єктивних та суб'єктивних факторів, що мають вражаючі властивості.

У той же час будь-яка безпека не може розглядатися знеособлено через те, що небезпека, яка проявляється в результаті актуалізації загроз, може бути породжена кимось або чимось, тобто потенційним зловмисником і одночасно спрямована на щось або когось – об'єкт. Однак в окремих джерелах (*Каламбет, Воронай, 2009*) питання знеособленості безпеки знімається, оскільки пропонується її розуміти як стан захищеності життєво важливих інтересів особистості, суспільства та держави від зовнішньої та внутрішньої загрози.

Така широка інтерпретація терміна «безпека» призводить до існування як мінімум трьох альтернативних назв науки про безпеку, яка зустрічається в навчальній та науковій літературі: «безпеказнавство», «економічна безпека», «сек'юрітологія». Проте загалом розуміння безпеки зводиться до наступних визначень (рис. 1).

Сказане вище свідчить, що питання безпеки багатогранні і можуть розглядатися з позиції філософії, соціології, політології, юриспруденції. Однак у рамках нашого дослідження увагу сконцентруємо на економічній безпеці. Результати аналізу спеціальної економічної літератури свідчать, що загальноприйнятого визначення економічної безпеки не існує, оскільки вітчизняні та зарубіжні вчені розглядають її сутність із різних сторін: від стану захищеності інтересів до здатності забезпечити вільний та незалежний розвиток суб'єкта. Аналіз дефініцій поняття «економічна

безпека» демонструє, з одного боку, актуальність та багатоаспектність досліджуваного поняття, а з іншого – показує вектор та масштаб розвитку думок вчених у досліджуваній проблематиці.

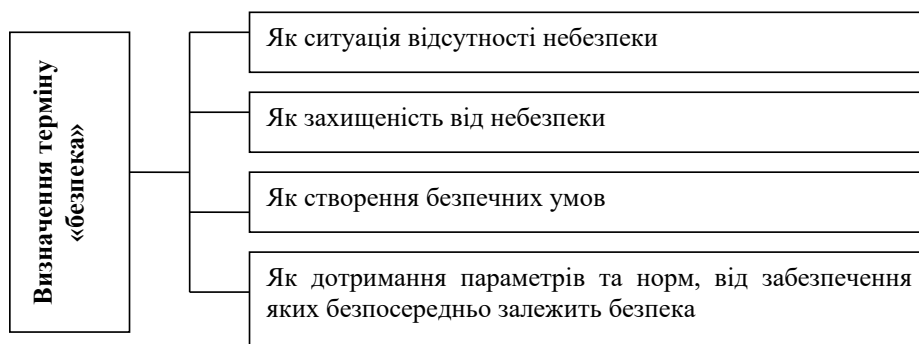


Рис. 1. Систематизація визначень терміну «безпека»

Водночас відсутність загальноприйнятої дефініції поняття «економічна безпека» і загалом підходу до розуміння її суті цілком логічно, що є наслідком звернення уваги вчених на різні рівні економічної системи. Незважаючи на те, що підприємницька діяльність виступає сполучною ланкою між усіма рівнями економіки, дослідження більшою мірою приділяються мезо- та макrorівню, що, безумовно, призводить до розвитку теорії та збагачення практики, але й збільшує розрив між ними як на рівні окремого підприємства, так і окремих галузей.

За своєю сутністю економічна безпека являє собою синтез економічної та політичної категорій, безпосередньо пов'язаною з економічною незалежністю, стабільністю та суверенітетом суб'єктів. Початково в практиці господарювання економічна безпека пов'язувалась із створенням умов забезпечення комерційної таємниці компаній, тому питання економічної безпеки полягали в забезпеченні надійності системи захисту корпоративної інформації, по-перше, за рахунок функціонування служби безпеки, по-друге, шляхом відповідальності співробітників щодо збереження комерційної таємниці. Такий підхід був неповним і полягав лише в забезпеченні захисту конфіденційної інформації підприємства, не враховуючи вплив зовнішніх факторів, які є важливим аспектом роботи компаній. Тому розуміння поняття економічної безпеки доповнилося новим змістом.

Так, М. М. Шкільняк висловлює точку зору, що економічна безпека корпорації – це захищеність від потенційних зовнішніх і внутрішніх економічних погроз, що впливають на незалежність і стійкість розвитку (Шкільняк, 2014). Однак, при цьому відсутнє чітке поняття цих загроз, критеріїв та їх взаємозв'язку із розвитком корпорацій. Деякі науковці дотримується іншої точки зору, вважаючи, що економічна безпека компанії – це стан, при якому негативні зміни зовнішнього середовища не можуть суттєво вплинути на параметри його майна та пов'язані з тимчасовими змінами (Мазаракі, 2010). Також існує позиція, що сутність поняття економічної безпеки являє собою мінімізацію втрат та збереження контролю над власністю (Гаркуша, 2018).

Узагальнення наведених визначень дозволяють систематизувати підходи до визначення терміну «економічна безпека корпорації» наступних чином (рис. 2).

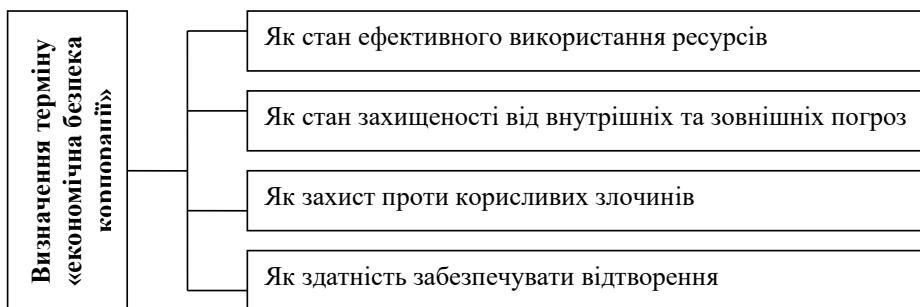


Рис. 2. Інтерпретація поняття «економічна безпека корпорації»

Економіко-управлінські питання щодо забезпечення економічної безпеки корпорацій досліджувалися переважно в працях зарубіжних вчених, зокрема Р. Найта, М. Стоуна, Р. Манна, М. Пауера, Ф. Рейнхарда, та інших. В іноземних публікаціях з початку ХХІ століття проблеми забезпечення економічної безпеки корпорацій стали досліджуватися в основному з позицій корпоративного ризик-менеджменту. В цілому, можна відзначити, що в роботах сучасних вітчизняних вчених мало розглядаються питання забезпечення економічної безпеки з точки зору економіко-управлінських аспектів забезпечення корпоративних структур. Дослідження переважно сфокусовані на інформаційно-технічних питаннях, які відносяться до служби безпеки компанії. При цьому економічна безпека виступає складовою всієї системи захисту компанії, стан системи захищеності всіх корпоративних бізнес-процесів. В даному аспекті не можна погодитись, що повноваження забезпечення економічної безпеки повинні покладатися лише на службу безпеки компанії, вони повинні поширюватися на керівників усіх підрозділів сучасних корпорацій: економістів, юристів, аудиторів, ризик-менеджерів, маркетологів тощо.

Зараз забезпечення економічної безпеки є важливим аспектом успішного функціонування та економічного розвитку корпоративних структур, що впливає на ефективність їх діяльності. Пріоритетним завданням забезпечення економічної безпеки корпоративних утворень в сучасному світі є створення передумов для стабільної та ефективної їх діяльності, динамічного зростання, формування потенціалу сталого розвитку корпоративних структур в перспективі. Раціональне використання всіх ресурсів компанії, важливих для їх діяльності, може бути досягнуто за рахунок зниження впливу негативних факторів на економічну безпеку корпорацій, що вимагає розробки та проведення спеціальної політики економічної безпеки, яка полягає у забезпеченні стабільної діяльності, зростанні фінансово-економічних показників, впровадженні інновацій, соціальному розвитку в умовах створених організаційно-правових та виробничих зв'язків та наявних інтелектуальних ресурсів.

Важливим компонентом економічної безпеки є ефективне корпоративне управління, яке являє собою певний спосіб якісного та кількісного об'єднання речових та трудових елементів виробничих процесів. Повне використання потенційних можливостей підвищення ресурсовіддачі та продуктивності праці

визначає ефективність економічної безпеки. Ефективне функціонування, підвищення конкурентоспроможності продукції, забезпечення та збереження пропорцій використання ресурсів, а також підвищення рівня корпоративного управління дозволяє гарантувати високий рівень активності бізнесу та його економічної безпеки.

Економічна безпека показує рівень фінансового потенціалу компанії, при якому господарський суб'єкт здатний забезпечити ефективний процес виробництва і реалізації продукції при оптимальному його використанні. Тому, економічна безпека компаній взаємопов'язана з корпоративним управлінням і фінансовою стійкістю.

Корпоративне управління економічною безпекою корпорацій, на нашу думку, слід вважати послідовністю дій суб'єкта управління над об'єктом управління, з метою розвитку економічної та фінансової діяльності компаній відповідно до забезпечення економічної безпеки. Здатність компанії адаптуватися підкреслює роль економічної безпеки в умовах зміни зовнішнього середовища при збереженні конкурентоспроможності та ефективності діяльності. При розгляді корпоративної структури як єдиної системи, ефективність діяльності можлива лише за умови злагодженої роботи всіх елементів, які необхідні для реалізації поставлених цілей і завдань. Корпоративним управлінням забезпечуються вимоги для оптимального використання основних елементів виробництва в просторі та часі.

Комплекс управлінських функцій, які є взаємозалежними між собою, передбачає існування певного нормативу для кожної функції окремо, встановлені значення якого визначають інтенсивність виконання функцій. При формуванні фінансової діяльності корпоративних структур функції можуть видозмінюватися, внаслідок чого змінюються й нормативи цих функцій.

Можна виділити чотири типи механізмів, за допомогою яких усуваються порушення функцій фінансово-економічної діяльності корпорацій, зокрема це механізми резервування, збереження, регулювання та подолання. Так, при порушенні нормального рівня економічної безпеки, включаються механізми резервування – це найвищий рівень економічної безпеки, в режимі подолання кризових явищ виникає необхідність у додаткових ресурсах (табл. 1).

Таблиця 1

Механізми управління економічною безпекою корпорації

Механізм	Відхилення від норми	Рівень економічної безпеки	Характеристика
Резервування	Позитивне відхилення від норми	Високий	Наявність надлишкової безпеки, відбувається резервування ресурсів
Збереження	Не перевищує граничне значення	Нормальний	Активна дія захисних механізмів, посилюється дія регулятивних механізмів, доводиться витрачати додаткові ресурси для підтримки рівноваги
Регулювання	Перевищує граничне значення	Низький	Компанія підтримує діяльність за рахунок додаткових ресурсів, зберігаючи життєво важливі елементи, знижується надійність функції
Подолання кризи	Перевищення можливостей регуляторного механізму	Критичний, необхідні додаткові ресурси	Виснаження ресурсів, суттєве відхилення від норми, може відбутися банкрутство компанії

Механізм регулювання є дієвим до тих пір, поки не перевищується рівень нарощування або зниження інтенсивності функцій управління. При цьому стан корпорації відноситься до низького рівня економічної безпеки, що для системи управління означає необхідність вдосконалення фінансової та економічної діяльності та залучення додаткових джерел для нормального функціонування.

Оскільки корпоративні структури потребують систематичної реорганізації та змін у системі управління, визначальним є створення нових ефективних ресурсів, спрямованих на подолання кризових явищ в межах ситуаційного управління. Тобто управління економічною безпекою є ситуаційним видом управління в компанії. Отже, забезпечення економічної безпеки компанії – це система, що включає в себе комплекс організаційно-управлінських, техніко-технологічних, режимних, а також профілактичних заходів, які спрямовані на якісний захист корпорації та її інтересів.

Політика економічної безпеки в корпоративному управлінні вимагає комплексного підходу, здійснення якого є досить складним, хоча і дуже важливим в умовах глобалізації, діджиталізації та інших сучасних тенденцій. Основним завданням політики економічної безпеки в корпоративному управлінні є забезпечення сталого та максимально ефективного розвитку компаній, виходячи із вищезазначених тенденцій, а також створення високого потенціалу зростання корпорацій в майбутньому. Політика економічної безпеки спрямована на забезпечення стабільного і динамічного розвитку, постійного балансування та гармонізації діяльності, які досягаються з використанням всіх типів доступних корпорації ресурсів і можливостей.

Формування і реалізація політики економічної безпеки відбувається через процес створення внутрішньокорпоративної системи економічної безпеки, орієнтованої на виявлення точок біфуркації в розвитку (трансформації зі стабільного стану корпоративного управління у нестабільний). Недостатня увага питанням політики економічної безпеки в корпоративному управлінні в значній мірі відбивається на результатах діяльності, динаміці зростання та сталому розвитку компаній.

Концепція економічної безпеки в корпоративному управлінні є системою певних поглядів та установок, спрямованих на вирішення проблеми забезпечення безпеки компанії, а також комплексом напрямків, заходів і пріоритетів для досягнення основних завдань корпорацій в умовах конкуренції та невизначеності, а також впливу зовнішніх і внутрішніх ризиків та загроз.

Процеси господарської діяльності корпорацій знаходиться в прямій залежності від рівня корпоративного управління. Виробництво може функціонувати виходячи із специфіки діяльності та обраної галузі, може бути сконцентрованим, маючи різні форми комбінування, що безпосередньо впливає на результати діяльності. Концептуальні положення формування політики економічної безпеки повинні, на наш погляд, включати в себе установчу, аналітичну та програмну складові, які є взаємозалежними та пов'язаними між собою.

Установчий елемент передбачає розробку місії, бачення, цілей і завдань, а також принципів політики економічної безпеки в корпоративному управлінні. Аналітичний елемент концептуального положення включає в себе визначення показників та індикаторів, а програмна складова передбачає створення методології оцінки політики економічної безпеки в корпоративному управлінні та механізмів забезпечення її ефективної реалізації.

Основною метою створення політики економічної безпеки в корпоративному управлінні при розробці концепції є забезпечення динамічного розвитку компанії на перспективу, з урахуванням негативних проявів зовнішнього і внутрішнього середовища. Для досягнення поставленої мети потрібно виявити відповідний вплив ризиків і загроз, а також оцінити стан і тенденції пріоритетного розвитку компанії з метою досягнення стратегічних показників політики економічної безпеки.

При проведенні аналізу різних концепцій щодо політики економічної безпеки корпорацій демонструється, по-перше, різноманітність понятійного апарату безпеки, по-друге, різноманіття існуючих методичних підходів. Розробка концептуальних підходів політики економічної безпеки в корпоративному управлінні, на нашу думку, повинна ґрунтуватися на принципах формування ефективного механізму, спрямованого на стійке зростання показників розвитку компанії. В економічній літературі не існує єдиного підходу до визначення основних принципів забезпечення політики економічної безпеки. Автори часто розглядають принципи однобоко, відсутній системний підхід до політики економічної безпеки в корпоративному управлінні. Так, на думку М.П. Мальської, економічна безпека базується на принципах взаємодії, узгодженості, реальності і практичної реалізації, визначенні прийнятного рівня ризику, комерційної та економічної ефективності (Мальська, 2012).

Розроблені та затверджені ОЕСР принципи корпоративного управління є основними для компаній, але вони не відображають підходів до політики економічної безпеки в менеджменті. У даних принципах особлива роль відводиться структурі корпоративного управління, яка повинна забезпечувати права акціонерів, повне розкриття інформації про фінансово-господарську та корпоративну діяльність, ефективний контроль тощо. За нашим переконанням, при розробці політики економічної безпеки в корпоративному управлінні необхідно ґрунтуватися на більш глобальному підході, зокрема пропонується наступна класифікація принципів політики економічної безпеки в корпоративному управлінні (рис. 3).



Рис. 3. Класифікація принципів політики економічної безпеки в корпоративному управлінні

В якості основних принципів політики економічної безпеки в корпоративному управлінні пропонується розглядати гармонійне поєднання:

- законності та документування – співвідношення напрямків економічної безпеки та нормативно-правової системи, що обумовлює відповідність дій політики економічної безпеки в корпоративному управлінні внутрішнім правовим документам та положенням;

- стабільності та динаміки структури компанії, що призводить до дотримання взаємозв'язків корпоративної структури, забезпечення існуючих структур, а також формування нових в умовах впровадження інновацій;

- раціональності та ефективності, що полягає в розширенні повноважень персоналу, з урахуванням оптимізації основної діяльності. При цьому витрати на проведення політики економічної безпеки компанії можуть варіювати, більш важливим є моніторинг результату і витрат в реалізації політики економічної безпеки в корпоративному управлінні;

- незалежності та колегіальності, який визначає раціональну самостійність та активність персоналу. Забезпечення економічної безпеки, на наш погляд, є результатом роботи колективу щодо формування напрямків політики економічної безпеки компанії, яка здійснюється всією командою;

- конфіденційності та захисту інформації, що полягає в забезпеченні комерційної таємниці, що визначає важливість політики економічної безпеки компанії в цілому;

- попередження та передбачення різних факторів, що негативно впливають на діяльність компанії. На наш погляд, цей принцип є найголовнішим, оскільки він спрямований на визначення зовнішніх і внутрішніх загроз;

- системності та безперервності – формування системи безпеки допомагає захистити майно та інші ресурси компанії в умовах конкуренції;

- перспективності та прогнозування – передбачає обґрунтування діяльності компанії з урахуванням існуючих тенденцій стану економічної безпеки компанії і прогнозів на майбутнє, спрямованих на реалізацію цілей і завдань, поставлених стратегією розвитку компанії.

Для формування ефективної політики економічної безпеки в корпоративному управлінні необхідно, в першу чергу, визначити рівень економічної безпеки на основі комплексного підходу і методів, спрямованих на підвищення результатів діяльності корпорацій та ефективності корпоративного менеджменту для об'єктивно необхідних інноваційних перетворень. У зв'язку з цим особливої актуальності в рамках даного дослідження набуває вибір необхідних критеріїв та показників оцінки економічної безпеки на корпоративному рівні.

У корпоративному управлінні критерій ефективності полягає в рівні реалізації місії компанії. В основу оцінки корпоративного управління прийнято закладати неокласичний, інституціональний та управлінський підходи. Так, неокласична теорія обґрунтовує існування можливостей отримання прибутку на базі технологічної ефективності, вона спрямована на оптимізацію різних виробничих факторів, необхідних для розвитку компаній, з метою досягнення максимального ефекту шляхом збільшення обсягів виробництва та зниження витрат.

Інституційна теорія на корпоративному рівні орієнтована на визначення витрат, їх нижнього та верхнього рівня, обґрунтування оптимального обсягу виробництва та встановлення критичних значень кількісних показників. Управлінські теорії поєднують теорію передачі повноважень, теорію зацікавлених осіб, поведінкові теорії корпорацій. Даний підхід заснований на визначенні різних цілей корпоративного управління, а не на максимізації доходу. Основою управлінських теорій є прагнення нарощування активів, а не збільшення прибутку, оскільки мотивація менеджерів залежить від розміру компанії.

Основним критерієм політики економічної безпеки в корпоративному управлінні, на наш погляд, повинна бути оцінка стану фінансово-економічної діяльності компанії: використання трудового потенціалу; матеріально-ресурсне забезпечення; фінансова незалежність; конкурентоспроможність; рівень інновацій та інформатизації. Встановити єдиний показник оцінки ефективності неможливо, оскільки результат діяльності корпорацій залежить від технологічних процесів, фінансового стану, впровадження інновацій, конкурентного поля, інформаційного та кадрового забезпечення. Одним з найбільш ранніх досліджень щодо показників економічної безпеки є робота початку XX століття У. Пірсона, який розробив так званий показник економічної кон'юнктури. Ця теорія отримала подальший розвиток у наукових працях У. Мітчелла (*Mitchell, 1051*), зараз вона широко використовується Національним бюро економічних досліджень в США.

Завданнями визначення рівня економічної безпеки в корпоративному управлінні є необхідність передбачення загроз і визначення напрямків розвитку. За допомогою системи кількісних індикаторів можна заздалегідь визначити поточний стан змін, що відбуваються в компанії, що дозволить своєчасно розробити сукупність дій щодо їх попередження.

Від правильності вибору системи показників для моніторингу економічної безпеки в корпоративному управлінні залежить ступінь точності оцінки забезпечення економічної безпеки компанії, комплекс заходів щодо запобігання і попередження ризиків і загроз. Виходячи з проведеного огляду наукової літератури, слід зазначити, що всі автори відносять до показників економічної безпеки виключно показники фінансово-господарської діяльності, та не враховують показники ефективності корпоративного управління. На наш погляд, визначальними індикаторами оцінки корпоративного управління є незалежність, відповідальність, прозорість і права власників. Отже, для моніторингу економічної безпеки корпорацій можна запропонувати наступну систему показників ефективності (табл. 2).

Таблиця 2

Система показників ефективності економічної безпеки корпорацій

Напрямки оцінки	Показники
1	2
Оцінна вартість компанії	- вартість акціонерного капіталу, - рентабельність, - економічна додана вартість
Показники фінансового стану компанії	- розмір прибутку, інвестований капітал, - рентабельність активів, - ділова активність компанії
Нефінансові показники	- обсяг виробництва, витрати на інновації,

	- конкурентоспроможність компанії
Витратні показники	- частка витрат у вартості продукції, - відповідність витрат нормам і нормативам, - темпи зростання витрат, - питома вага неефективних витрат
Показники корпоративного управління	- незалежність (зовнішній аудит, відсутність одноособного власника, незалежні директори), - відповідальність (оптимальна кількість та рівень відповідальності членів ради директорів, прозорість структури, соціальна відповідальність), - прозорість (звітність перед акціонерами), - права власників (виборчість органів управління, інформування про збори).

Аналіз оцінки рівня економічної безпеки корпорацій дозволяє визначити ефективність діяльності всіх структурних підрозділів та ступеню їх захищеності. Для визначення оцінки рівнів економічної безпеки необхідна оперативна оцінка параметрів, що визначають захищеність компанії. Взаємозв'язок між елементами системи оцінки рівнів економічної безпеки наведена в табл. 3.

Таблиця 3

Багаторівнева система оцінки економічної безпеки корпорацій

Рівні оцінки	Напрямки оцінки	Система показників	Методи
I рівень	Оцінка економічної безпеки	- дані управлінського обліку; - дані фінансового обліку.	- аналіз; - синтез; - експертні оцінки.
II рівень	Показники взаємодії	Ефективність використання: - оборотних активів; - трудових ресурсів; - фінансової та інвестиційної діяльності; - імідж компанії.	- порівняльний аналіз; - угруповань; - оцінки взаємозв'язку індикаторів економічної безпеки.
III рівень	Показники оперативної оцінки	- ризик фінансово-господарської діяльності; - платоспроможність компанії.	- стохастичний аналіз; - регресійний та дисперсійний аналіз.
IV рівень	Узагальнюючі показники	- вартість компанії	- порівняльний аналіз; - прогнозування; - експоненціального згладжування.

Пропонована система оцінки дозволяє визначити рівні оцінювання економічної безпеки компанії, що складається з комплексу відповідних методів. Головним показником оцінки рівня економічної безпеки компанії в пропонованій методиці є оцінка вартості компанії, що визначається на основі коригування балансової вартості капіталу на показники, що характеризують економічну незалежність компанії та захищеність економічних інтересів її власників.

При формуванні концепції політики економічної безпеки в корпоративному управлінні необхідний комплексний підхід, що враховує зміни рівня фінансового стану

на основі узагальнюючого критерію та оцінки рівня економічного розвитку компанії. Критичні значення індикаторів економічної безпеки характеризуються переліком факторів виробничого та соціально-економічного характеру, які проявляються в активності, а також в граничних значеннях зниження рівня економічної безпеки, масштабах виробництва та інших факторах, за межами яких не представляється можливим подальший розвиток корпорації. Концептуальні підходи до економічної безпеки корпорацій ґрунтуються на урахуванні зовнішніх та внутрішніх загроз, які тісно пов'язані з рівнем розвитку компанії, регіону та країни в цілому.

Для забезпечення економічної безпеки корпорацій традиційно застосовуються наступні функціональні стратегії безпеки (табл. 4).

Таблиця 4

Система показників ефективності економічної безпеки корпорацій

Назва стратегії	Зміст стратегії
Стратегія економічної безпеки	Включає систему превентивних заходів, реалізується через регулярну, безперервну роботу всіх підрозділів корпорації з перевірки контрагентів, аналізу передбачуваних угод, експертизі документів, виконання правил роботи з конфіденційною інформацією і т. п. В ролі контролера в даному випадку виступає служба економічної безпеки.
Стратегія реактивних заходів	Застосовується у разі виникнення або реального здійснення будь-яких загроз економічної безпеки корпорації. Ця стратегія, заснована на застосуванні ситуаційного підходу і врахуванні всіх зовнішніх і внутрішніх чинників, реалізується службою економічної безпеки через систему заходів, специфічних для даної ситуації.

Тактика забезпечення економічної безпеки припускає застосування конкретних процедур і виконання конкретних дій з метою забезпечення економічної безпеки корпорації (Зачосова, Філяр, 2017).

Таким чином, для ефективного розвитку корпоративного управління головним є забезпечення економічної безпеки компанії, яке передбачає створення багатогранної концепції формування політики економічної безпеки. Запропоновані концептуальні підходи дозволяють проводити діагностику рівнів економічної безпеки компанії на основі цілісного методу, що дозволить глибоко вивчити стан та тенденції розвитку фінансово-економічної діяльності компанії.

2. Види та інструменти комплаєнсу для забезпечення економічної безпеки корпорацій

Комплаєнс сьогодні є одним з найсучасніших трендів, що активно розвиваються. На відміну від зарубіжних (особливо західних) компаній, де цей напрямок активно розвивається вже кілька десятиліть, вітчизняне корпоративне управління з цією функцією зіткнулося порівняно недавно. Одна з головних причин виникнення до теми інтересу, на наш погляд, полягає у виході українських компаній на міжнародні фінансові ринки, де важливою умовою для запозичення є наявність прозорості, успішно функціонуючої комплаєнс-системи та ефективного управління нею. Інкорпорування нової функції потребує наявності відповідної законодавчої бази, формування якої вже відбувається у вітчизняному правовому полі. Але перш, ніж аналізувати статус даного процесу, слід розібратися, що це за явище і звідки воно виникло.

Необхідно відзначити, що у вітчизняній науці цей напрямок, незважаючи на досить значну кількість вже прийнятих у його розвиток та чинних нормативно-правових актів, знаходиться у початковій стадії розробки, тому знайти наукове визначення явища – досить непросте завдання. Вікіпедія з посиланням на оксфордський словник англійської мови визначає compliance як «дію відповідно до запиту або вказівки; послух» (англ.: *compliance is an action in accordance with a request or command, obedience*). Тобто, термін «комплаєнс» означає відповідність будь-яким внутрішнім або зовнішнім вимогам або нормам, маючи на увазі дотримання чинного законодавства (зовнішні вимоги) та внутрішніх правил компанії. На наш погляд, дане тлумачення виглядає дещо спрощено, проте воно відображає суть явища загалом і цілком може бути відправною точкою для подальших досліджень.

Єдиної думки щодо термінологічного визначення комплаєнсу немає. Наприклад, представники банківського сектора, які першими зіткнулися з цим явищем ще на початку «нульових», визначають комплаєнс як здатність діяти відповідно до інструкцій, правил та спеціальних вимог (Гаврікова, 2012). У банківській сфері поширеним є розуміння комплаєнсу як складової частини функції внутрішнього контролю, метою якої є захист інтересів інвесторів, банків та їх клієнтів шляхом контролю за дотриманням співробітниками банку положень чинного законодавства, вимог наглядових органів, а також документів, що визначають внутрішню політику та процедури банку, в чому, власне, і полягає суть банківського комплаєнса (Калініченко, 2016).

Термін «комплаєнс-контроль» у банківському регулюванні вперше був введений Базельським комітетом у квітні 2005 року у виданому документі «Комплаєнс та комплаєнс-функція в банках», в якому комплаєнс-контроль визначено як внутрішній контроль за відповідністю діяльності банківської установи на фінансових ринках законодавству про фінансові ринки у загальній системі внутрішнього контролю банку. Також у зазначеному документі визначено наступні основні принципи комплаєнсу в банках (рис. 4).

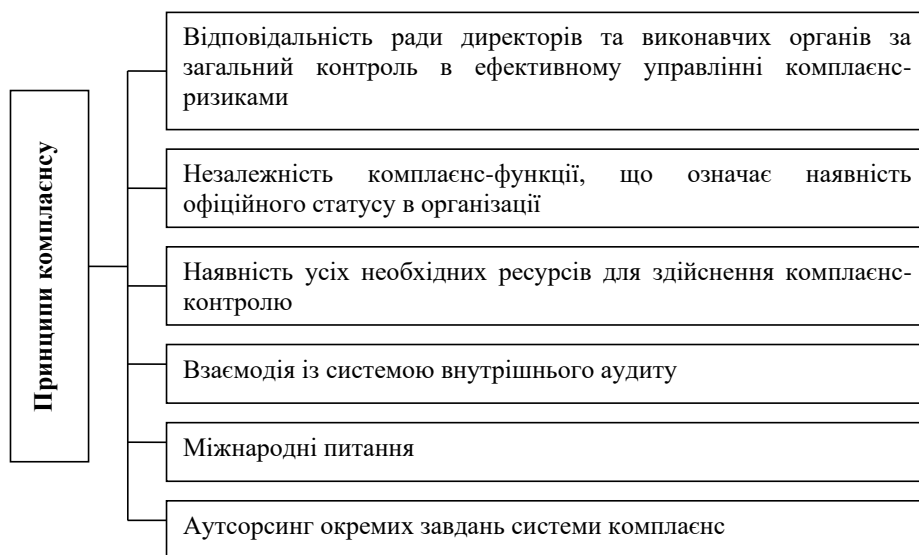


Рис. 4. Принципи комплаєнс-контролю

Слід зазначити, що мета комплаєнсу в банках є достатньо вузькоспрямованою і полягає у запобіганні несанкціонованим операціям з грошовими коштами, протидії «відмиванню» грошей, тобто легалізації незаконно отриманих доходів та фінансуванню терористичних організацій. Саме тому комплаєнс у банках орієнтований в основному на проведення контрольних заходів. Подальше поширення комплаєнсу на інші сфери економіки, а також законодавчий розвиток явища потребували уточнення як самого терміну, так і закладених у комплаєнс принципів та процедур.

Незважаючи на відсутність поняття «комплаєнс» у тлумачних словниках, воно міцно увійшло у ділове середовище, закріпившись у професійному лексиконі фахівців із найрізноманітніших сфер та індустрій: банківському секторі, оподаткуванні, антимонопольному законодавстві та стратегічному консалтингу та т.ін. Етимологічно, як зазначалося вище, слово «комплаєнс» походить від англійського слова «compliance». Суворо кажучи, це поняття не є науковим терміном і в англійській мові, що підтверджується, зокрема, його відсутністю у таких авторитетних наукових словниках англійської мови, як Oxford Dictionary та Barron's Law Dictionary.

У сучасному корпоративному управлінні термін «комплаєнс» використовується в різних сферах, але в цілому його зміст майже завжди зводиться до дотримання (як правило, добровільного) встановлених у законодавстві та інших нормативно-правових та внутрішньокорпоративних актах норм та правил. У професійній спільноті менеджерів термін «комплаєнс» використовується досить давно. Крім того, в мережі «Інтернет» присутня значна кількість оглядів, статей, інших робіт та документів вітчизняних та міжнародних аудиторських та консалтингових фірм, у яких цей термін також досить широко використовується.

Необхідно визнати, що у вітчизняній науці дослідження комплаєнсу, незважаючи на більш ніж десятирічний період його фактичного застосування, знаходиться на початковому етапі, що створює певний дефіцит вагомих наукових праць та монографій. При цьому слід відзначити наявність до даної тематики значного інтересу, що підтверджується великою кількістю присвячених комплаєнсу наукових та практичних статей, в яких термін «комплаєнс» використовується без перекладу, і це цілком зрозуміло, оскільки україномовний аналог «відповідність» не відображає глибину змісту, що вкладається в нього, і, як правило, вимагає додаткового тлумачення.

Говорячи про розвиток комплаєнсу, не можна не торкнутися глибинних витоків його виникнення, одним з яких, як нам здається, є мораль (корпоративна етика), а іншим – право, закон (система правил та встановлених норм). Відповідно, формування та підтримання збалансованого співвідношення моралі та закону в суспільстві дозволяє ефективно регулювати практично всі сфери його життя та діяльності з тим, щоб скоротити кількість фактів несправедливого та неправомірного трактування та використання діючих у суспільстві установ та правил. Крім того, мораль і закон нерідко йдуть пліч-о-пліч, позначаючи межі дозволеного, формуючи саме розуміння правомірної (як і неправомірної) поведінки, що безпосередньо впливає на створення законодавчої бази всередині соціуму, що дозволяє йому повноцінно існувати, діяти і визначати подальший розвиток.

Саме усвідомлена потреба соціуму у формуванні та розвитку правових засад суспільства стала, на наш погляд, причиною появи як комплаєнсу в цілому, так і його окремих видів та інструментів, визначила їхнє послідовне практичне застосування, заклала фундамент для створення нормативної бази кожного з існуючих видів комплаєнсу. З цієї позиції, комплаєнс – це комплекс ініціатив, спрямований на попередження дій співробітників компанії, що суперечать закону, та впровадження корпоративної бізнес-етики, заснованої на дотриманні законодавчих та локальних актів.

Також комплаєнс визначається як система внутрішнього контролю, яка дозволяє управляти комплаєнс-ризиками: ризиками притягнення до відповідальності компаній та топ-менеджерів, і заснована на системному попередньому контролі за подіями, які можуть призвести до недотримання встановлених вимог та зобов'язань.

На думку Т.О. Кобелевої (*Кобелева, 2019*), корпоративний комплаєнс являє собою сукупність процедур (процесів) економічного суб'єкта, що регламентують поведінку персоналу щодо дотримання законодавчих та етичних норм. Розглядаючи комплаєнс здебільшого з позиції внутрішнього контролю, авторка зазначає, що до його процедур обов'язково слід включати:

- протидію корупції, управління конфліктом інтересів, а також регулювання процесу прийняття та дарування подарунків, запрошень на різні світські та розважальні заходи;
- протидію відмиванню доходів, отриманих злочинним шляхом, та фінансуванню тероризму;
- забезпечення каналів зворотного зв'язку для повідомлень про порушення законодавчих та етичних стандартів;
- нерозголошення даних, що стосуються конфіденційної інформації в організації;
- організацію зберігання та дотримання певних стандартів при обробці персональних даних тощо.

В цілому, як у теорії, так і на практиці комплаєнс трактується як зведення законодавчих, професійних та етичних норм і правил, як загального характеру, так і сформованих у кожній компанії індивідуально, але при цьому обов'язкових для дотримання всіма працівниками приватних, державних та громадських структур незалежно від їх становища в ієрархії.

За різними оцінками в корпоративній практиці налічується понад сотні видів комплаєнсу, що з достатнім ступенем упевненості дозволяє говорити про високу затребуваність даного напрямку діловою спільнотою та про увагу дослідників, якої комплаєнс заслуговує. На нашу думку, значна частина із зазначеної кількості видів комплаєнсу складається з унікальних систем, створених відповідно до конкретних бізнес-умов, що ставить під сумнів необхідність їх детального дослідження. Дані системи представляють інтерес, в основному, для практикуючих комплаєнс-фахівців. Досвід показує, що існує досить обмежений набір універсальних видів комплаєнсу, на які тією чи іншою мірою орієнтується будь-який бізнес, які максимально ефективно забезпечують економічну безпеку в системі корпоративного управління (рис. 5).

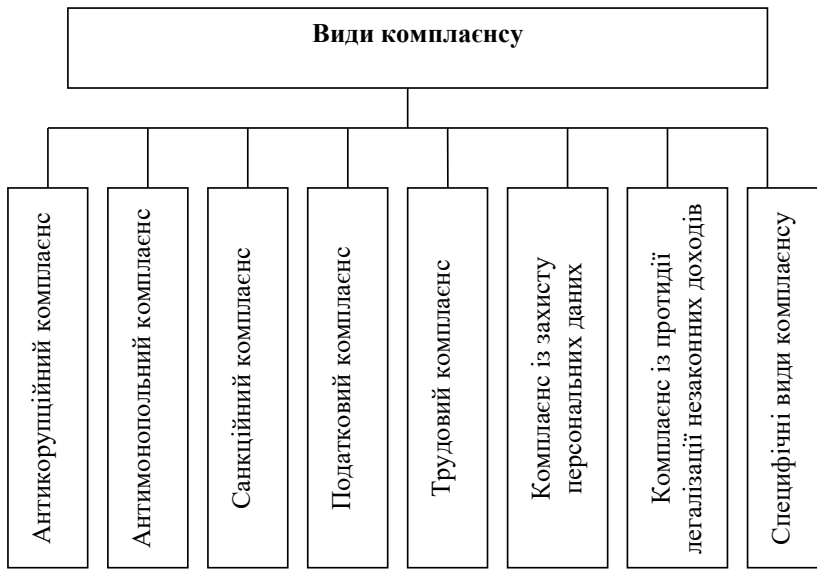


Рис. 5. Види комплаєнсу в корпоративному управлінні

Зупинимося на цих видах докладніше.

1. *Антикорупційний комплаєнс* є найбільш поширеним та вельми значущим напрямом, пов'язаним з протидією існуючим на практиці зловживанням чиновників і комерційних керівників різного рівня своїм службовим становищем. Інструментарій антикорупційного комплаєнсу спрямований не лише на запобігання корупції всередині корпорації, а й на її виявлення. Віднести до корупційних фактів можна будь-які протиправні дії, які здійснюють співробітники корпорації як у своїх власних інтересах, так і в інтересах третіх осіб. У зв'язку з цим особлива увага в рамках антикорупційного комплаєнсу, як правило, приділяється запобіганню та врегулюванню конфлікту інтересів.

Інструментарій антикорупційного комплаєнсу на корпоративному рівні полягає у визначенні системи локальних нормативних актів, у яких мають бути описані внутрішні антикорупційні правила та механізми контролю. Форму таких актів не регламентовано, проте певні вимоги при їх складанні мають бути враховані, а саме:

- визначення підрозділів або посадових осіб, відповідальних за профілактику корупційних та інших правопорушень;
- співробітництво корпорації з правоохоронними органами;
- наявність чинних стандартів та процедур, спрямованих на забезпечення сумлінної роботи корпорації;
- прийняття кодексу етики та службової поведінки працівників корпорації;
- запобігання та врегулювання конфлікту інтересів;
- недопущення складання неофіційної звітності та використання підроблених документів.

2. *Антимонопольний комплаєнс*. Слід зазначити, що антимонопольне законодавство розвивається та контролюється державою в особі антимонопольної служби для регулювання конкурентного характеру ринкового ціноутворення та відносин між різними юридичними особами у певних економічних умовах. Дія

антимонопольного законодавства поширюється на всіх учасників процесу: виробників, посередників та споживачів. У зв'язку з цим основною метою регулювання для антимонопольного комплаєнсу є запобігання вільному ринку узгоджених дій, які можуть призвести до отримання необґрунтованих доходів його суб'єктами та завдати шкоди споживачам. Проте, практика показує, що антимонопольний комплаєнс може застосовуватися щодо всіх сфер, де є контроль з боку антимонопольного регулятора. Це насамперед роздрібна торгівля, реклама, ЖКГ, державні закупівлі, оборонні замовлення, окремі види біржової торгівлі.

В даний час на експертному рівні обговорюється питання про розпізнавання незаконної активності контрагентів і конкурентів та протидію їй шляхом її включення до поняття антимонопольного комплаєнсу. При цьому поява нових сфер контролю в полі зору антимонопольного комплаєнсу неминуче призведе до додаткових витрат на їх регулювання для всіх учасників ринку, тоді як помірні та низькі витрати на реалізацію заходів у рамках антимонопольного комплаєнсу неминуче призведуть до його популяризації у всіх сферах бізнесу.

3. *Санкційний комплаєнс.* Цей вид комплаєнсу увійшов у ділову сферу відносно недавно, хоча на практиці застосовується вже протягом значної кількості часу. Говорити про необхідність його дотримання конкретною корпорацією можна лише тоді, коли вона здійснює зовнішньоекономічну діяльність у країнах та на територіях, включених до списків санкцій. Витоки санкційного комплаєнсу відносять до США, коли для окремих юридичних осіб, особливо для транснаціональних корпорацій, виникла потреба перевіряти контрагентів, які могли перебувати під санкціями ООН або іншими міждержавними обмеженнями, щоб виключити можливість бути штрафованими на значні суми за порушення умов санкційних режимів.

В даний час у зв'язку зі значним збільшенням кількості територій, що знаходяться під санкціями, юридичних та фізичних осіб, роль цього виду комплаєнсу значно зросла. Необхідність відстежувати санкційні зміни в режимі «нон-стоп», моніторити законодавчі новели на міжнародному та локальному рівні змушує корпорації створювати окремі структури санкційного комплаєнсу, щоб оперативно коригувати свою діяльність у стрімких умовах.

Продуманий та чітко структурований комплаєнс має володіти всіма сучасними правовими інструментами, щоб ефективно та своєчасно здійснювати дії щодо запобігання та мінімізації санкційних наслідків з дотриманням законодавчих вимог на всіх рівнях їх формування.

Західна санкційна практика має набагато давніший характер. Вона сформована законодавчими актами США (FCPA, FATCA, GAATSA), Великобританії (UKBA), ЄС, Швейцарії та ін. Документи, що приймаються державами, визначають параметри та правила санкційного комплаєнсу для корпорацій, які ведуть бізнес у різних країнах, включаючи і ті, що входять до санкційних списків.

Слід зазначити, що санкційний режим США має свої особливості, до яких, наприклад, належить «правило 50%» («50% Rule» - Entities Owned by Persons Whose Property and Interest in Property are Blocked). Це правило означає, що санкційні обмеження поширюються не тільки на фізичних та юридичних осіб, які перебувають у списках SDN (пряма заборона на будь-які форми співробітництва) та SSI (секторальні санкції, що вводять ряд обмежень, проте не забороняють деякі форми

співробітництва), але й на компанії, що прямо або опосередковано належать одному або декільком подібним особам на 50 і більше відсотків. Як наслідок, у рамках санкційного комплаєнсу необхідна та проводиться повна перевірка контрагентів за всіма санкційними списками, включаючи їх зв'язки та кінцевих бенефіціарів угод.

Управління з контролю за іноземними активами (OFAC) Міністерства фінансів США штрафує порушників санкційних режимів незалежно від галузі та обсягів угоди з особами, які перебувають у SDN-списках. Розмір штрафів варіюється від десятка тисяч до мільярдів доларів. Серед галузей бізнесу переважно компанії фінансового сектора схильні до високих ризиків.

Широке поширення в санкційних обмеженнях набули так звані «вторинні санкції», які можуть бути накладені на компанії, які прямо і побічно не підпадають під конкретні рестрикції, але вступають у договірні відносини з об'єктами первинних санкцій. Це правило збільшує ризики для всіх учасників міжнародних правовідносин, а відсутність конкретних регулюючих документів щодо детального розшифрування та застосування санкційних режимів сприяє зростанню правової невизначеності у цьому питанні.

4. *Податковий комплаєнс.* Даний вид знаходиться біля витоків зародження всього комплаєнсу як самостійного спрямування. Саме ухвалення Податкового кодексу як спроба структурування досить запутаного податкового законодавства призвело до появи послуги, пов'язаної з впровадженням податкового комплаєнсу у комерційних структурах на корпоративному рівні. Значні податкові донарахування, штрафи та пені в ході успішних податкових перевірок породили попит на податкове консультування, призвели до виникнення у практичному обігу терміну «податковий менеджер», так само як і окремого спрямування в комплаєнсі та в системі економічної безпеки в цілому.

З деяким ступенем умовності податковий комплаєнс можна поділити на:

- поточний, при якому комплаєнс-підрозділ (служба економічної безпеки або внутрішнього аудиту) регулярно перевіряє договори, а за окремими, найбільш значними угодами (наприклад, придбання нерухомості) проводить юридичне дослідження всіх правових питань, включаючи оподаткування;

- періодичний, у якому детально розглядається певний етап роботи компанії. Як правило, цей період становить 2-3 роки, оскільки саме цей термін найчастіше потрапляє до зони податкової перевірки. На даному етапі завданням служби економічної безпеки є аналіз змін податкового законодавства та оцінка рівня їх застосування в організації;

- проектний, коли комплаєнс-підрозділ (служба економічної безпеки або внутрішнього аудиту) допомагає перевірити чистоту угоди, наприклад, з продажу часток у статутному капіталі корпорації покупцю та підготувати поточному власнику компанію до продажу;

- постфактичний, коли комплаєнс-підрозділ (служба економічної безпеки або внутрішнього аудиту) визначає, чи всі правові ризики були враховані при угоді і чи є необхідність у проведенні певних коригувальних процедур.

5. *Трудовий (кадровий) комплаєнс.* Цей вид комплаєнсу нерозривно пов'язаний із трудовим законодавством, яке з початку 2000-х років і дотепер бурхливо розвивалося

і продовжує вдосконалюватися. Перманентні правові зміни у нормативно-правових актах трудової спрямованості призводять до питань, що закономірно виникають у процесі практичного застосування трудового законодавства.

Слід зазначити, що всі існуючі нестикування у трудовому законодавстві в переважній більшості випадків трактуються на користь найманого працівника. Щоб нівелювати негативні наслідки, роботодавці формують Правила внутрішнього трудового розпорядку та застосовують їх у взаємозв'язку зі стандартною формою трудових договорів. Цей комплект внутрішньої документації, оформлений та введений у чинність відповідно до вимог Кодексу законів про працю, створює основу функціонування трудового комплаєнсу на рівні корпорації.

Штатна чисельність, за якої рекомендується використання трудового комплаєнсу, законодавчо не зафіксована. Лише на експертному рівні вона визначена у 200 осіб, проте необхідність у трудовому комплаєнсі може виникати і за меншої кількості персоналу. Така необхідність визначається обсягом трудової документації та операцій, які лягають на спеціаліста з кадрів, юриста, безпосереднього менеджера.

Безумовно, кадрове адміністрування потребує регулярного моніторингу. Організація та здійснення такого моніторингу, як правило, реалізується комплаєнс-підрозділом або, за відсутності останнього, службою економічної безпеки спільно з відділом персоналу. Також, на практиці зустрічаються й інші способи реалізації трудового комплаєнсу, як, наприклад, здійснення комплаєнс-контролю лінійними менеджерами або залучення зовнішніх спеціалістів.

Однак, не у всіх корпораціях застосування трудового комплаєнсу є необхідним та можливим. Наприклад, у невеликих компаніях, де діяльність практично всього персоналу перебуває під постійним контролем керівництва, наявність окремого підрозділу та наділення його особливими повноваженнями є недоцільним. Тим не менш, це не звільняє корпоративне керівництво від необхідності дотримуватись вимог чинного трудового законодавства.

Насправді система трудового комплаєнса може функціонувати у кількох варіантах:

- розподіл посадових обов'язків між відділом персоналу, юристами та службою охорони праці;
- покладання комплаєнс-контролю на лінійних керівників;
- створення окремого комплаєнс-підрозділу, яке забезпечуватиме виключно трудові аспекти бізнесу;
- залучення зовнішніх фахівців, що також є ефективним методом впровадження трудового комплаєнсу.

Ускладнений процес розірвання трудових відносин спонукає корпоративне управління чіткіше формулювати вимоги Правил внутрішнього трудового розпорядку та спиратися на значну кількість кадровиків та юристів відповідного профілю. З іншого боку, ці самі фактори спонукають роботодавця активно розвивати трудовий комплаєнс, спрямовувати ресурси на формування корпоративної культури, всіма доступними способами підвищувати рівень лояльності працівників.

6. *Комплаєнс із захисту персональних даних.* Цей вид комплаєнсу також виник порівняно недавно і передбачає насамперед обмеження доступу до особистої

інформації про клієнтів та співробітників компанії, а також обов'язкове отримання від будь-яких фізичних осіб, пов'язаних з діяльністю конкретної корпорації, згоди на обробку та використання цих даних у діяльності компанії.

7. *Комплаєнс із протидії легалізації незаконних доходів.* Особливе значення в умовах обмежень щодо руху капіталу сьогодні приділяється комплаєнсу, пов'язаному з протидією легалізації незаконних доходів, або, іншими словами, «антивідмивним» практикам. Порушення жорстких вимог валютного та «антивідмивного» законодавства з високою ймовірністю може призвести до блокування рахунків та паралізувати всю діяльність компанії. Відповідно, велике значення набувають процедури перевірки платіжних документів і самих контрагентів, а також операцій щодо їх оцінки з позиції комплаєнсу із протидії легалізації незаконних доходів. Зневажливе ставлення до зазначених вимог, і тим більше їхнє повне ігнорування може змусити банк до запиту нових уточнюючих документів, що призведе, у кращому випадку, до затримки оплати, а в гіршому – до її повної зупинки з подальшою більш пильною увагою з боку банку, не кажучи вже про ймовірні штрафи. Деталі інформації, що надається у відповідь на банківський запит, можуть бути настільки глибокими, наскільки це взагалі можливо, щоб уникнути блокування.

Інші види комплаєнсу, як зазначалося вище, визначаються досить вузькими специфічними обставинами, у зв'язку з чим їх детальний аналіз у даному дослідженні не проводиться.

У процесі впровадження комплаєнс-системи в компаніях з різною організаційно-правовою формою виникає низка закономірних питань щодо загальної доцільності комплаєнсу, його критеріїв та форм, в яких він може бути реалізований у структурі корпоративного управління, рівнів керівництва, на яких він має бути представлений. Так, виходячи з чинного законодавства, наявність комплаєнс-системи є обов'язковою для публічних акціонерних товариств, чії акції знаходяться у відкритому обігу. Це суттєва вимога та умова допуску до торгів абсолютно всіх біржових інститутів, що існує незалежно від їхньої територіальної приналежності та ринків, в рамках яких вони функціонують.

Що стосується непублічних компаній, то питання організації та впровадження комплаєнс-системи в їхню структуру залишається відкритим. На нашу думку, кожне акціонерне товариство, що має статус приватного (ПрАТ), повинне підходити до вирішення цього питання індивідуально. Для приватних акціонерних товариств, які мають дочірні структури, використання комплаєнс-системи можна вважати обов'язковою умовою, оскільки вони управляються з єдиного центру і повинні дотримуватись єдиних вимог законодавства.

На наш погляд, створення ефективно функціонуючої комплаєнс-системи в непублічних компаніях – це один з основних факторів формування внутрішньої основи економічної безпеки існуючої корпоративної системи. Основу комплаєнсу має формувати єдина внутрішня система нормативних актів, що визначають моделі та правила поведінки співробітників у різних ситуаціях з урахуванням інтересів, вимог та правил, встановлених роботодавцем. Крім того, створення комплаєнс-системи у приватних акціонерних товариствах є обов'язковим щодо протидії корупції на підставі відповідного антикорупційного законодавства.

Наступним після ухвалення відповідного рішення етапом буде вибудовування комплаєнс-системи на практиці, коли велике значення має досвід розробки та впровадження локальних нормативно-правових актів, а також створення практичних інструментів їх функціонування. Головним тут буде формулювання основних постулатів, цінностей та правил, які матимуть однакову правову силу для всіх працівників незалежно від їх посади, територіального розташування, покладених обов'язків та розв'язуваних завдань.

Насамперед необхідно зафіксувати ті правила, наявності яких потребує чинне законодавство, як національне (для всіх організацій, що діють на території країни), так і міжнародне (актуально для транснаціональних компаній та груп). Зміст та необхідність запровадження додаткових правил, які можуть визначатися характером внутрішніх умов діяльності, кожна корпорація визначає самостійно.

Набір внутрішніх правил може бути різним залежно від особливостей функціонування корпорації, яка його розробляє. Проведене дослідження дозволяє сформулювати набір таких особливостей (критеріїв), які можна подати у наступному вигляді (рис. 6).

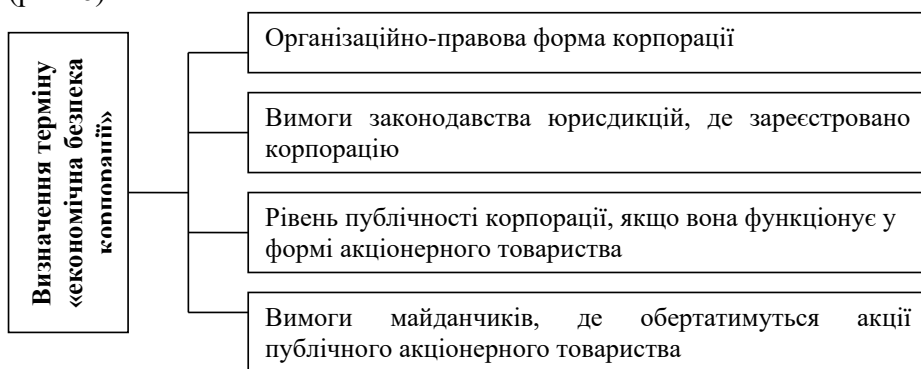


Рис. 6. Особливості, що визначають набір внутрішніх правил корпоративного управління

Для кожної із зазначених вище груп та компаній може бути прийнятий свій регламент, який з урахуванням перелічених нами критеріїв визначить необхідний набір документів, порядок навчання, характер процесів, розподіл виконавчих та контрольних функцій, характер, склад, періодичність складання та рівень подання звітності. Як правило, звітність щодо виконання внутрішніх правил у публічних компаніях складається щорічно та включається до структури корпоративного звіту, який затверджується річними зборами акціонерів.

Одним із найважливіших питань, пов'язаних з ефективним функціонуванням комплаєнс-системи незалежно від організаційно-правової форми компанії є відповідальність. З цієї позиції відповідальність за дотримання встановлених внутрішніх правил лежить не тільки і не стільки на комплаєнс-функції, як такий і не на конкретному комплаєнс-менеджері, який виконує цю функцію, а на кожному працівнику компанії, починаючи від простих фахівців і закінчуючи вищим керівництвом. При цьому відповідальність за організацію та ефективну роботу системи має нести найвище керівництво. Цим визначається так званий «тон-зверху», тобто пряма зацікавленість вищого керівництва та власників компанії у дотриманні

встановлених внутрішніх правил усіма її співробітниками. Комплаєнс-функція в будь-якій структурі повинна відповідати за відповідність встановлених комплаєнс-системою правил вимогам чинного законодавства, їх своєчасну актуалізацію та обґрунтованість, розуміння та чітке усвідомлення необхідності дотримання встановлених правил усіма членами трудового колективу.

Таким чином, основною метою комплаєнсу в корпоративному управлінні є виключення або мінімізація ймовірної шкоди внаслідок запобігання порушенням чинного законодавства шляхом встановлення додаткових захисних механізмів превентивної дії у формі законодавчо обґрунтованих внутрішніх нормативних документів корпорації.

У рамках досягнення поставлених перед нею цілей комплаєнс-система вирішує наступні завдання:

- організація та забезпечення ефективної комунікації чинних внутрішніх правил усім співробітникам компанії;
- регулярне навчання співробітників чинним внутрішнім правилам у координації з відділом персоналу;
- оцінка розміру та ймовірності виникнення шкоди, можливої внаслідок порушень чинних правил, а також координація, контроль та юридичний супровід розслідувань у разі їх порушення;
- консультування керівництва та всіх працівників компанії з правових та процесуальних питань у частині встановлених внутрішніх правил, визначення легітимних та прийнятних дій;
- організація та підтримка каналів зворотного зв'язку, необхідних для інформування (у тому числі й анонімного) про скоєні порушення встановлених внутрішніх правил;
- розробка та погодження внутрішніх документів (положень, інструкцій та окремих видів договорів), які уточнюють чинні правила або формують нові вимоги;
- підготовка звітності щодо дотримання встановлених внутрішніх правил (як мінімум, у щорічному форматі) та кооперація з усіма функціями та керівництвом з поточних питань їх адаптування та дотримання.

Яким чином комплаєнс-функція буде вбудована в загальну систему корпоративного управління, вирішується кожною корпорацією індивідуально, виходячи з конкретної ситуації та завдань, що стоять перед бізнесом. Однак, у всіх випадках важливо, щоб комплаєнс-підрозділ, що забезпечує функціонування системи, повинен бути достатньо незалежним. Щоб забезпечити достатній рівень незалежності комплаєнс-підрозділу у структурі корпоративного управління, його слід безпосередньо підпорядковувати виконавчому органу компанії. При цьому для комплаєнс-підрозділу має бути створена можливість виходу на наступний рівень (наприклад, на власників компанії), якщо порушення правил допущені представниками виконавчого органу.

На практиці комплаєнс-підрозділ існує або як самостійна одиниця, або він вбудований у структуру юридичного відділу, який найчастіше підпорядковується генеральному директору у приватних акціонерних товариствах або незалежному члену ради директорів, якщо мається на увазі публічна компанія. У деяких компаніях

комплаєнс-підрозділ може входити до структури служби економічної безпеки, однак, дана схема має, на нашу думку, більше недоліків, ніж переваг.

Важливим інструментом є організація та проведення відповідного навчання працівників чинним внутрішнім правилам. В даному аспекті комплаєнс-підрозділ обмежений лише межами власних компетенцій та фінансовими можливостями конкретної корпорації. Законодавство не регламентує формати навчання, що застосовуються, а також не забороняє залучення зовнішніх фахівців для його проведення. Єдине законодавче обмеження існує для навчання з охорони праці та техніки безпеки в рамках трудового законодавства, яке визначає необхідність залучення спеціалістів із відповідним чином ліцензованих організацій.

Навчання корпоративним нормам організується у двох загальнодоступних та досить широко поширених формах: особиста присутність працівника та електронне навчання на робочому місці. Навчання у формі особистої присутності для новоприйнятих працівників, як правило, щомісяця організується відділом персоналу та проводиться комплаєнс-підрозділом. Організація та контроль електронного навчання в цілому по компанії, а також навчання у формі особистої присутності в окремих структурних підрозділах – цілком і повністю відповідальність відділу персоналу. Проте комплаєнс-підрозділ має забезпечити кадрову службу усіма матеріалами, необхідними для проведення навчання. Акцент під час проведення навчання у будь-якій формі робиться на обговорення конкретних комплаєнс-ситуацій, пов'язаних із практичним застосуванням встановлених у компанії внутрішніх правил.

На навчанні у формі особистої присутності рекомендується застосовувати інтерактивне залучення працівників до обговорення кожного випадку виявлених порушень. Також корисною буде практика використання відео, аудіо та інших матеріалів, наприклад, мультфільмів за затвердженими правилами, безпосередніх звернень керівництва з теми навчання, вікторин, практичних пояснень юристів з конкретних вимог законодавства (наприклад, антимонопольних правил) та ін. Всі ці прийоми з урахуванням об'єктивних складнощів у сприйнятті юридичних текстів роблять навчання цікавим та легко сприйманим.

Електронне навчання новоприйнятих працівників у частині чинних внутрішніх правил рекомендується провести протягом 3-6 місяців після навчання у формі особистої присутності. Таке навчання не залежить від організаційно-правової форми компанії та є обов'язковим для всіх співробітників, якщо комплаєнс-система вже впроваджена та діє. Це дозволяє освіжити раніше отриману інформацію про встановлені правила та закріпити її у свідомості працівників. Організація навчання спеціальним темам у рамках окремо взятих вимог (антикорупційна, антимонопольна, за персональними даними тощо) здійснюється аналогічно. Як додаткові форми навчання можна використовувати бесіди за корпоративними нормами з окремими працівниками та підрозділами. Розклад таких розмов рекомендується заздалегідь узгоджувати з членами ради директорів компанії і проводити безпосередньо представниками комплаєнс-підрозділу.

Одним із важливих напрямків роботи підрозділу з дотримання корпоративних норм є оцінка ризиків їх порушення, яка повинна проводитись регулярно з використанням різних сценаріїв (корупція, конфлікт інтересів, антимонопольні

правила, дискримінація, відмивання незаконних доходів, шахрайство та ін.). В якості основних форм рекомендується використовувати як інтерактивні семінари, так і індивідуальні інтерв'ю. Кожна з цих форм має свої переваги та недоліки. Наприклад, переваги семінару полягають у можливості обговорити наявні ризики недотримання чинних внутрішніх правил з керівниками різних рівнів, переконатися у розумінні керівниками цих ризиків, допомогти розібратися в них та визначити заходи щодо їх зниження. Недоліками цієї форми є часові розриви, які не дозволяють окремим керівникам брати участь у заході, а також обмежений час його проведення, що значно звужує коло ризиків, що обговорюються. Тоді як індивідуальні бесіди з кожним керівником дають можливість детально обговорити всі можливі в його підрозділах ризики порушення встановлених правил та індивідуальні для кожного підрозділу заходи щодо їх запобігання.

Значна роль у перевірці дотримання внутрішніх правил належить аудиторам організації. В рамках аудиторських процедур здійснюється контроль за дотриманням встановлених правил, виявляються випадки їх порушення за підсумками опитувань та аналізу документів. Інформація щодо виявлених порушень, як правило, направляється в комплаєнс-підрозділ для її подальшої оцінки та визначення кроків та заходів щодо запобігання подібним порушенням надалі. Незважаючи на те, що в процесі аудиту перевіряються історичні дані та виявляються інциденти, що вже відбулися, його результати використовуються для коригування встановлених правил, приведення їх у відповідність чинному законодавству, виявлення можливостей їх оптимізації та необхідності у проведенні додаткового навчання співробітників.

Окремим інструментом контролю комплаєнс-системи є зовнішній аудит, який важливий для власників з позиції дотримання вимог чинного законодавства не тільки на національному, а й на міжнародному рівні, і дозволяє оцінити її правомірність, а також відповідність правовим параметрам діяльності компанії, визначеним умовами чинного законодавства.

Важливим інструментом ефективного функціонування системи корпоративних норм є лінія зворотного зв'язку, яка може бути реалізована декількома способами, як, наприклад: спеціально виділена лінія телефонного зв'язку, окрема скринька електронної пошти, окреме посилання на сайті. При цьому компанії можуть як вибрати будь-який із зазначених способів, так і застосовувати їх одночасно. У неопублічних компаніях організація, первинна обробка та відстеження повідомлень, що надійшли по лінії зворотного зв'язку, віддається, як правило, безпосередньо комплаєнс-підрозділу або службі безпеки. Однак у публічних компаніях управління повідомленнями, що надійшли за зворотним зв'язком, передається незалежному оператору. Ця умова необхідна для того, щоб забезпечити передачу в комплаєнс-підрозділ абсолютно всієї інформації, що надійшла, повністю виключивши можливість її коригування або видалення зацікавленими особами.

Лінія зворотного зв'язку повинна бути розміщена як у внутрішній комунікаційній системі для співробітників компанії, так і в загальному доступі для клієнтів, постачальників та підрядників на сайті компанії. Крім того, звернення, пов'язані з порушенням встановлених внутрішніх правил, можуть надходити і іншими каналами, призначеними, наприклад, для прийняття скарг від споживачів у зв'язку з порушенням їх прав, а також через розміщені в соціальних мережах

сторінки, відгуки на електронних торгових майданчиках, особисті звернення до керівництва. Щоб не втратити подібну інформацію, комплаєнс-підрозділ може розробити та направити відповідальним співробітникам список критеріїв (наприклад, ключових слів), наявність яких у зверненні автоматично робить його обов'язковим для направлення до комплаєнс-підрозділу з подальшою оцінкою та організацією відповідної перевірки.

Комунікація про підсумки розгляду звернень, що надійшли на лінію зворотного зв'язку, також є дуже важливою. Вона дає співробітникам орієнтири правильних та правомірних дій, демонструє непримиренність компанії до порушень встановлених внутрішніх правил та вимог чинного законодавства.

Отже, необхідність впровадження комплаєнс-системи залежно від організаційно-правової форми компанії та територіального розташування майданчика визначається на всіх рівнях чинного законодавства, починаючи від міжнародних вимог та закінчуючи національними правилами.

Висновок. Дослідження термінологічного плюралізму думок у науковому дискурсі дозволило встановити, що за своєю сутністю економічна безпека являє собою синтез економічної та політичної категорій, безпосередньо пов'язаною з економічною незалежністю, стабільністю та суверенітетом суб'єктів.

Важливим компонентом економічної безпеки є ефективне корпоративне управління, яке являє собою певний спосіб якісного та кількісного об'єднання речових та трудових елементів виробничих процесів. Повне використання потенційних можливостей підвищення ресурсівддачі та продуктивності праці визначає ефективність економічної безпеки. Ефективне функціонування, підвищення конкурентоспроможності продукції, забезпечення та збереження пропорцій використання ресурсів, а також підвищення рівня корпоративного управління дозволяє гарантувати високий рівень активності бізнесу та його економічної безпеки. Для формування ефективної політики економічної безпеки в корпоративному управлінні необхідно, в першу чергу, визначити рівень економічної безпеки на основі комплексного підходу і методів, спрямованих на підвищення результатів діяльності корпорацій та ефективності корпоративного менеджменту для об'єктивно необхідних інноваційних перетворень, у зв'язку з чим особливої актуальності набуває вибір необхідних критеріїв та показників оцінки економічної безпеки на корпоративному рівні.

Проведені дослідження дозволили сформулювати визначення комплаєнсу як зведення законодавчих, професійних та етичних норм і правил, як загального характеру, так і сформованих кожною корпорацією індивідуально, але при цьому обов'язкових для дотримання всіма працівниками приватних, державних та громадських структур незалежно від їх положення.

Зроблено загальний висновок про те, що формування комплаєнс-системи корпорації безпосередньо залежить від її організаційно-правової форми, а публічність або непублічність компанії є одним із основних факторів, що визначають необхідність створення та ефективного функціонування комплаєнсу в її організаційній структурі.

References:

- Братчук У.П. Фінансовий комплаєнс як інструмент удосконалення фінансової архітектури. *Економіка і організація управління*. : 2023. № 3 (51). <https://doi.org/10.31558/2307-2318.2023.3.2>
- Гаркуша В.О., Єршова Н.Ю. Теоретичні та методичні підходи до організаційного забезпечення економічної безпеки підприємства. *Економіка і суспільство*. 2018. № 18. С. 333 – 339. DOI: <https://doi.org/10.32782/2524-0072/2018-18-46>
- Зачосова Н.В., Фімяр С.В. Економічна безпека суб'єктів господарювання. *Інноваційні підходи до забезпечення безпеки України: макро та мікрорівні*. Черкаси, 2017. С.158-171. URL: <https://eprints.cdu.edu.ua/879/1/cherevko2017.pdf>
- Каламбет С.В., Воропай В.А. Підходи до трактування економічної безпеки підприємства. URL: <http://ekuzt2009.detut.edu.ua/sekcziya-3-lekonomika>
- Калініченко Л.Л. Теоретичні аспекти функціонування комплаєнсу у вітчизняних банках. URL: http://www.ej.kherson.ua/journal/economic_06/250.pdf.
- Кобелева Т.О. Комплаєнс-безпека промислового підприємства: теорія та методи. Харків, 2019. – 354 с. URL: <https://repository.kpi.kharkov.ua/items/e97ecca7-d94a-4b8b-904c-72c9f36e3cb3>
- Мазаракі А.А. Економічна безпека України в умовах глобалізаційних викликів: монографія / Мазаракі А.А, Мельник Т.М., Бохан А.В., Головня Ю.І. та ін. Київ, 2010. 660 с. ISBN 978-966-629-463-3
- Мальська М.П. Корпоративне управління: теорія та практика. Київ, 2012. 360 с. ISBN 978-611-01-0343-5
- Польова, Н., Когут Р., Дума Ю. Напрями забезпечення безпеки підприємства в умовах цифровізації бізнесу. *Розвиток міста*, 2024. № 1. С. 90–94. DOI 10.32782/city-development.2024.1-12
- Принципи корпоративного управління «Групи 20» і ОЕСР. URL: <http://https://globalcentre.hse.ru/nletter7.7>
- Шкільняк М.М. Корпоративне управління. Тернопіль: Крок, 2014. 293 с. URL: <http://dspace.tneu.edu.ua/handle/316497/25355>
- Mitchell W.C. What happens during business cycles. N.Y., 1951. URL: <https://www.nber.org/system/files/chapters/c4759/c4759.pdf>

CHAPTER 10. TAX POTENTIAL FOR FORMING LOCAL BUDGET REVENUES

Valentyna GLUKHOVA

PhD in Economics, Associate professor
Associate professor of the Department of Accounting and Finance,
Kremenchuk Mykhailo Ostrohradskyi National University,
(20, University Street, Kremenchuk, 39600, Ukraine)

Glukhova710@gmail.com
<https://orcid.org/0000-0003-3120-9651>

Abstract. In the conditions of a full-scale war, crisis phenomena in the economy, centralized budget resources in Ukraine are limited both at the national and local levels. The foundation of local budget revenues is tax revenues, therefore it is important to form them taking into account the tax base that is maximally possible in a particular territory. It is precisely for these purposes that the tax potential of local budget revenues serves, which is the basis for forecasting, planning tax revenues, identifying and using their reserves. Therefore, the issues of studying the tax potential of local budget revenues are relevant, and all its components: realized, unrealized and forecasted.

The paper considers the theoretical foundations of the tax potential of local budget revenues. The dynamics, structure of its realized component in relation to the revenues of local budgets of Ukraine, trends and reasons for changes and the possibility of growth due to improving the tax base, rates, administration mechanism, especially local taxes and fees, are analyzed in detail.

The unrealized component of tax potential was studied in detail using the available information base. It was determined that this component is characterized by under-receipt and losses of tax revenues due to the provision of tax benefits, tax debt and tax evasion through the shadow economy. Ways of improving the unrealized component in the formation of tax revenues of local budgets were proposed.

Keywords: tax potential, local budget revenues, taxes, realized and unrealized tax potential, local taxation, tax benefits.

ПОДАТКОВИЙ ПОТЕНЦІАЛ ФОРМУВАННЯ ДОХОДІВ МІСЦЕВИХ БЮДЖЕТІВ

Анотація. В умовах повномасштабної війни, кризових явищ в економіці централізовані бюджетні ресурси в Україні є обмеженими як на загальнодержавному, так і на місцевому рівнях. Фундаментом доходів місцевих бюджетів є податкові доходи, тому важливо їх формувати з урахуванням такої бази оподаткування, яка є максимально можливою на тій чи іншій території. Саме цим цілям і слугує податковий потенціал формування доходів місцевих бюджетів, який є основою прогнозування, планування податкових доходів, виявленню та використанню їх резервів. Тому питання дослідження податкового потенціалу доходів місцевих бюджетів є актуальними, причому всіх його складових: реалізованої, нереалізованої та прогнозованої.

В роботі розглянуто теоретичні основи податкового потенціалу формування доходів місцевих бюджетів. Проаналізовано детально динаміку, структуру його реалізованої складової стосовно доходів місцевих бюджетів України, тенденції та причини змін і

можливості зростання за рахунок вдосконалення бази оподаткування, ставок, механізму адміністрування, особливо місцевих податків і зборів.

Досліджена детально за наявною інформаційною базою нереалізована складова податкового потенціалу. Визначено, що ця складова характеризується недоотриманням та втратами податкових доходів за рахунок надання податкових пільг, податкового боргу та ухилення від оподаткування через тіньову економіку. Запропоновано шляхи вдосконалення нереалізованої складової при формуванні податкових доходів місцевих бюджетів.

Ключові слова: податковий потенціал, доходи місцевих бюджетів, податки, реалізований і нереалізований податковий потенціал, місцеве оподаткування, податкові пільги.

Вступ. Формування фінансових ресурсів органів місцевого самоврядування в умовах децентралізації посилює значення використання податкових і бюджетних інструментів і важелів у соціально-економічному розвитку адміністративно-територіальних утворень. В цьому аспекті велику роль відіграє податковий потенціал місцевого самоврядування.

Визначальна роль у формуванні доходів місцевих бюджетів країни належить податковим надходженням. Саме фактичні податкові надходження свідчать про здатність і готовність органів місцевого самоврядування фінансувати бюджетні видатки. В кризових економічних і умовах воєнного стану в Україні посилюються диспропорції в соціально-економічному регіональному розвитку. Часті законодавчі зміни в податковій системі, зростання податкового навантаження на суб'єктів господарювання знижують підприємницьку активність, призводять до ухилення від оподаткування, що веде до недоотримання доходів місцевих бюджетів, створює загрози бюджетній та податковій безпеці територіальних громад, веде до розбалансування, дефіцитності бюджетів місцевого самоврядування.

Реальні та потенційні доходи місцевих бюджетів дає змогу визначити податковий потенціал, який виступає також інформаційною базою для прогнозування й планування податкових доходів місцевих бюджетів. Дослідження рівня податкового потенціалу та його кількісне оцінювання віддзеркалюють потенційну здатність територіальних громад утворювати податкові доходи бюджетів, яку варто всіляко використовувати для створення та нарощування доходів місцевих бюджетів, чим і відзначається актуальність теми.

Проблемами визначення суті та дослідження складових податкового потенціалу, пошук можливостей забезпечення податкових надходжень до бюджетів, вивчення методів його оцінки на регіональному рівні вітчизняні науковці займаються протягом тривалого періоду (А. Буряченко, 2016; С. Каламбет, 2003; Т. Канєва, М. Рубан, 2018; Т. Канєва, М. Карпенко, 2024; Д. Міщенко, А. Перетяцько, 2017; О. Мірчев, 2003; М.Олексій, 2024; Н. Педченко, 2011; Л. Тарангул, 2003; І. Цимбалюк, І. Редько, 2013; І. Цимбалюк, Д. Антонюк, М. Карлін, 2022 та інші). Однак важливо зазначити, що невирішених проблем стосовно податкового потенціалу формування доходів бюджетів територіальних громад на даний момент є чимало, що і зумовило вибір теми дослідження.

Метою роботи є поглиблення науково обґрунтованих положень та висновків, спрямованих на теоретичний та практичний аналіз податкового потенціалу України,

визначення проблемних аспектів і розроблення пропозицій по реалізації податкового потенціалу.

1. Теоретичні аспекти податкового потенціалу формування доходів місцевих бюджетів.

Формування фінансово спроможних адміністративно-територіальних утворень базового рівня в умовах децентралізації в Україні вимагає нарощування фінансово-економічного потенціалу територіальних громад.

Доходи місцевих бюджетів є фінансовою базою діяльності органів місцевого самоврядування, адже вони забезпечують виконання ними власних і делегованих повноважень. В умовах повномасштабної війни з РФ потреба у фінансових ресурсах в регіонах значно зростає. Основу доходів місцевих бюджетів без міжбюджетних трансфертів, традиційно формують податкові надходження. Тому податковий потенціал доходної бази місцевих бюджетів відіграє надзвичайно важливу роль.

Склад податків і зборів місцевих бюджетів в Україні визначається відповідно до статей 64 та 69 Бюджетного кодексу України, причому є особливості наповнення ними доходів бюджетів територіальних громад, обласних і районних бюджетів, що визначаються закріпленням і пропорціями розподілу між ланками бюджетної системи (*Бюджетний кодекс України: Закон України від 08.07.2010 р. № 2456– VI. URL: <http://zakon0.rada.gov.ua/laws/show/2456-17>*).

Місцеві бюджети – це фінансові плани, від правильності і повноти їх складання залежить фінансове забезпечення надання суспільних послуг в регіонах, розвиток територій. Оскільки податкові доходи є фундаментом місцевих бюджетів, тому важливо їх формувати з урахуванням такої бази оподаткування, яка є максимально можливою на тій чи іншій території. Саме цим цілям і слугує податковий потенціал формування доходів місцевих бюджетів, який є основою стратегічного бюджетного планування.

Категорія податкового потенціалу трактується у науковій літературі по-різному вченими:

- податковий потенціал як фактор, що визначає розміри податкових надходжень (*С.Каламбет, 2003*);

- податковий потенціал - максимально можлива величина потенційного ресурсу регіону, мобілізація та ефективне використання якої приведе до збільшення доходів бюджету та сприятиме соціально-економічному розвитку регіону (*Д. Міщенко, А. Перетяцько, 2017*).

Деякі вчені розмежовують податковий потенціал у вузькому і широкому аспектах. Так, Л. Тарангул вважає, що у вузькому розумінні - це такі фінансові ресурси, що підлягають мобілізації податкових платежів до бюджету згідно діючої системи оподаткування в країні (*Л.Тарангул, 2003*). В широкому сенсі податковий потенціал - це обсяг реальних і потенційних ресурсів регіону, які підлягають оподаткуванню, а також можуть бути об'єктом оподаткування при розширенні його податкової бази. Виходячи із таких припущень, Л. Тарангул започатковує сутнісні поняття реальної податкоспроможності, що відображає по факту податкові надходження місцевого бюджету на території певного регіону при визначеному рівні розвитку економіки, і потенційної податкоспроможності, тобто можливості відносно

мобілізації податкових доходів і зборів до бюджету із залученням всіх додаткових ресурсів (Л. Тарангул, 2003).

Виходячи з цього, автор робить висновок, що податковий потенціал регіону є не лише основою для оцінки обсягів надходжень потенційно податкових доходів до місцевих бюджетів, а й базою для фінансового вирівнювання розвитку регіонів, зокрема за їх рівнем податкоспроможності.

Отже, дослідження теоретичних основ податкового потенціалу свідчить, що він відображає не лише існуючий рівень оподаткування адміністративно-територіальних одиниць, але й резерви, що можна використати для вдосконалення механізму фінансового вирівнювання регіонів.

На нашу думку, податковий потенціал органів місцевого самоврядування як економічна категорія - це економічні відносини в територіальних громадах, що виникають у процесі пошуку всіх можливостей формування податкових доходів бюджету задля фінансового забезпечення потреб економічного, соціального розвитку, підвищення добробуту мешканців та ефективного оптимального перерозподілу дотримуючись принципу справедливості в процесі фінансового вирівнювання.

За змістом податковий потенціал являє прогностичний обсяг податків до місцевих бюджетів, який може бути сформований у взаємодії податкових органів та платників податків задля максимально можливого наповнення бюджетів територіальних громад фінансовими ресурсами та з урахуванням мінімально можливих втрат податкових доходів, в тому числі за рахунок недоотримання потенційних податків через податкові пільги, податковий борг, ухилення від оподаткування тощо.

Термін «податковий потенціал» пов'язаний із такими категоріями як «податкові ресурси» та «податкові можливості». Податкові ресурси – це сформована податкова база регіону, податкові можливості визначають імовірний рівень акумулювання податкових доходів при умові функціонування діючої податкової системи. Тому, звісно, поняття податкового потенціалу значно ширше, ніж податкові можливості й податкові ресурси.

Податковий потенціал доходів місцевих бюджетів доцільно також розглядати як суму потенціалів окремих податків і зборів, які надходять до бюджетів територіальних громад і які залежать від об'єктивних і суб'єктивних факторів впливу. Особливо це стосується місцевого оподаткування, яке в значній мірі залежить від діяльності органів місцевого самоврядування в нарощуванні економічної бази регіонів, створенні валового регіонального продукту та його розподілу в ході формування власних доходів місцевих бюджетів. Тому важливим є комплексний підхід, спрямований на посилення потенціалу як загальнодержавних, так і місцевих податків і зборів, і в результаті – зміцнення податкоспроможності регіону.

Основними джерелами формування податкового потенціалу доходної бази місцевих бюджетів є потенційні податкові надходження, податкові бази, ставки, реальні та потенційні можливості платників податків.

Характерні властивості податкового потенціалу формування доходів місцевих бюджетів можна окреслити наступним чином:

1) означає максимальний обсяг податків, який на основі розвитку ділової активності в територіальних громадах, можна акумулювати як основну складову доходів бюджету;

2) він обчислюється в межах регіону за певний проміжок часу;

3) передумовою максимуму отримання податкових доходів є оптимальне використання матеріальних, трудових, фінансових ресурсів у регіоні;

4) строга відповідність чинному податковому законодавству та врахування стратегій розвитку системи оподаткування в цілому, в тому числі й на місцевому рівні.

Отже, показник податкового потенціалу має велике значення та може використовуватися для різних цілей: для прогнозування, планування податкових доходів у місцеві бюджети; для визначення міжбюджетних трансфертів задля ефективного горизонтального фінансового вирівнювання на основі показників податкоспроможності адміністративно-територіальних одиниць; для виявлення резервів податкових надходжень до місцевих бюджетів.

Формування та реалізація податкового потенціалу доходів місцевих бюджетів потребує визначення і характеристики його складових. Варто зазначити, що у світовій практиці єдиного підходу до таких складових немає.

Більшість вітчизняних науковців виділяють три основні складові податкового потенціалу: реалізовану, нереалізовану та прогнозовану (рис. 1.1).

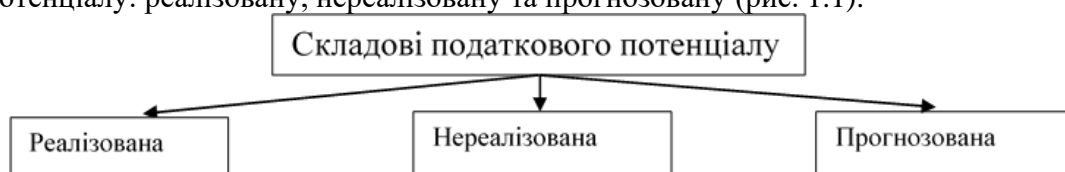


Рис. 1.1 Складові податкового потенціалу

Джерело: побудовано за даними (С.Каламбет,,2003)

Кожна складова містить свої джерела формування податкового потенціалу регіону. Найважливішою реальною складовою формування податкового потенціалу є реалізована складова, яка характеризує фактичні податкові доходи місцевих бюджетів. Мобілізація податків, зборів, обов'язкових платежів у повному обсязі до бюджетів становить реалізовану складову податкового потенціалу (Н. Педченко, 2011).

Реалізована складова утворюється з податкових надходжень до місцевих бюджетів. Дійсну базу оподаткування формують об'єкти оподаткування підприємницької діяльності; оподаткування доходів фізичних осіб, оподаткування споживання населенням суспільних благ, а також власності.

Зростання ставок і бази оподаткування призводить до розширення першої складової податкового потенціалу.

Податкові платежі формують в основному доходи місцевих бюджетів. Бюджетоутворюючими на місцевому рівні є такі податки і збори: податок з доходів фізичних осіб (ПДФО); єдиний податок; екологічний податок; місцеві податки і збори, які включають: податок на нерухоме майно, відмінне від земельної ділянки;

плату за землю; транспортний податок; податок на прибуток; рентна плата; акцизний податок; туристичний збір, збір за паркування автотранспорту.

Найважливішими елементами кожного із податків є: об'єкт податку, база оподаткування, ставка податку, платник, податковий період, порядок обчислення податку тощо, які визначаються в Податковому кодексі України (ПКУ). (ПКУ від 02.12.2010 № 2755-VI. URL(<http://zakon.rada.gov.ua/cgi-bin/laws/main.=275-17>)).

Нереалізована складова податкового потенціалу включає податкові пільги, податковий борг і розширену базу оподаткування, яка в свою чергу охоплює надходження від виходу з тіньової економіки, розширення податкової бази на наявних підприємствах, а також нові податки на наявні об'єкти.

Розглянемо більш детально деякі складові нереалізованого податкового потенціалу. Податкові пільги відіграють важливу роль в стимулюванні економічної діяльності суб'єктів господарювання, реалізації принципів соціальної справедливості стосовно фізичних осіб. Податкові пільги частково або повністю звільняють платника податків від їх сплати, відтермінують в часі строки сплати. Якщо для платників податкові пільги зменшують податковий тягар, то для держави в цілому, в тому числі і для місцевого самоврядування, вони спричиняють втрату податкових доходів.

Компенсація збитків від отримання податкових пільг для бюджетних доходів можлива шляхом прискорення соціально-економічного розвитку від їх застосування або шляхом виділення дотації з державного місцевим бюджетам на компенсацію недоотриманих доходів.

Таким чином, нереалізована складова податкового потенціалу у вигляді наданих податкових пільг зумовлює податкові видатки, тобто це сума недоотриманих податкових надходжень внаслідок застосування будь-якого положення податкового або митного законодавства, яке визначає податкову пільгу.

Оскільки податкові пільги спричиняють втрати доходів місцевого бюджету, вони є ризиком, що загрожує податковій безпеці, а в умовах воєнного стану не сприяють збалансованості бюджетів.

Вагомим складником податкових втрат бюджетних ресурсів органів місцевого самоврядування є втрати, пов'язані з неефективним управлінням податковим боргом. Відповідно до 14.1.175 п. 14.1 ст. 14 Податкового кодексу України, податковий борг – це сума узгодженого грошового зобов'язання, не сплаченого платником податків у встановлений строк, та непогашеної пені (ПКУ від 02.12.2010 № 2755-VI URL:<http://zakon.rada.gov.ua/cgi-bin/laws/main.=275-1>)).

Податковий борг свідчить про неузгодженість взаємовідносин платників податків і зборів з контролюючими органами щодо формування податкових доходів місцевих бюджетів. Податковий борг може виникати і через скрутне фінансове становище платників податків, загрози банкрутства.

Нереалізований податковий потенціал виникає також і через тінізацію економіки. Несплачені, недоотримані податки зменшують податкову базу надходжень у місцевих бюджетах, а це загострює проблему дефіциту бюджетних коштів в органах місцевого самоврядування. Тому досить важливо досліджувати детінізацію економіки як спосіб збільшення податкових надходжень до бюджетів базового рівня.

Загальновідомо, що тіньова економіка – це діяльність економічних суб'єктів, яка здійснюється поза межами державного обліку й контролю, а тому в офіційній статистиці не відображається. Відповідно, доходи від такої тіньової діяльності не обліковуються, а отже податки не сплачуються до бюджетів.

Наявність значних масштабів тіньової економіки в Україні спричинена багатьма факторами: неефективним державним регулюванням економіки; недосконалим інституційним та законодавчим забезпеченням у сфері оподаткування; неефективним адмініструванням податків, високим податковим навантаженням; відсутністю дієвої системи контролю і його результативності через неофіційне працевлаштування, неоподаткування заробітної плати; недосконалістю організації боротьби з організованою злочинністю, зокрема в економічній сфері та іншими.

Відповідно, нереалізована складова податкового потенціалу формування доходів місцевих бюджетів через тінізацію фінансових потоків збільшується внаслідок ухилення від оподаткування, мінімізації податкових зобов'язань, виведення фінансових ресурсів платників податків в офшорні зони, легалізації одержаних злочинним шляхом доходів. Звичайно, наразі існують проблеми через недостатність інформації в обчисленні цих складників нереалізованого податкового потенціалу, але вдосконалення організаційної, інформаційної, законодавчої та методичної роботи державних органів та спеціалізованих інститутів повинно бути спрямоване на розширення джерел формування доходів місцевих бюджетів саме за рахунок цієї складової, яка є вагомим резервом зростання їх податкових надходжень і доходів у цілому.

Отже, нереалізована складова податкового потенціалу формування доходів місцевих бюджетів характеризується втратами їх податкових надходжень за рахунок надання податкових пільг, податкового боргу та ухилення від оподаткування таких через тіньову економіку.

Прогнозована складова податкового потенціалу доходів місцевих бюджетів являє потенційну базу оподаткування, тобто можливі податкові надходження від економічного зростання в територіальних громадах і створення в них нових суб'єктів господарювання – потенційних платників податків.

Прогнозована складова податкового потенціалу відіграє дуже важливу роль при прогнозуванні та бюджетному плануванні.

Об'єктивність оцінювання податкового потенціалу доходів місцевих бюджетів залежить від вибору системи показників, методу оцінювання податкового потенціалу, адже це дасть можливість розробити заходи, які будуть спрямовані на збільшення податкових надходжень. В Україні та за кордоном використовуються різні методичні підходи до оцінювання податкового потенціалу доходів бюджетів органів місцевого самоврядування.

Це говорить про те, що єдиної системи оцінки податкового потенціалу немає, а використовуються ті методи, які найбільш прийнятні для країни і які забезпечені інформаційною базою для обчислень відповідних показників, причому вони можуть змінюватися в залежності від наповнення складових податкового потенціалу, векторних змін економічного та соціального розвитку адміністративно-територіальних утворень.

Взагалі існує дві групи методів визначення податкового потенціалу регіону,

зокрема: методи абсолютних і методи відносних величин. До першої групи відносять методи, за допомогою яких обчислюють податковий потенціал в абсолютному вимірі, розраховують суми фактичних чи прогнозованих податкових надходжень.

До другої групи методів відносяться такі, за якими розраховують відносні показники, а саме: співвідношення податкових надходжень до певних показників: метод на базі середнього доходу на одного мешканця громади; метод на основі макроекономічних показників (ВВП, ВРП); метод на основі індексу податкоспроможності регіону; метод на базі індексу податкового потенціалу (ІПП).

Розрахунок податкового потенціалу формування доходів місцевих бюджетів можна здійснювати на основі різних показників. Однак вибір оптимального методу оцінювання залежить від мети та завдань щодо аналізу формування податкового потенціалу територіальних громад. Для оцінювання податкового потенціалу регіонів України, зокрема доходної бази бюджетів територіальних громад, найбільш доцільним вважаємо метод із застосуванням індексу податкового потенціалу на основі ВРП. Використання цього методу дає можливість об'єктивно оцінити фактичні дохідні можливості кожного регіону порівняно зі стандартами.

Кількісні показники оцінювання податкового потенціалу доходної бази місцевих бюджетів можна доповнити деякими новими, які з 2021 року стали розраховуватися в Україні і відображатися на Дашборді в інтерактивному режимі («Дашборд «Бюджети територіальних громад України».[URL: https://decentralization.ua/finance/dashboard](https://decentralization.ua/finance/dashboard)). Зокрема, до них можна віднести:

- дохідність земель громади (визначається як співвідношення суми плати за землю до території громади) (тис. грн). Цей показник відображає, наскільки ефективно використовується земля територіальної громади, що виявляється у проведенні чіткої та повної інвентаризації земель, результативності адміністрування даного майнового податку місцевих бюджетів, проведенні обґрунтованої грошової оцінки землі;

- фіскальна віддача території, тобто співвідношення надходжень обсягів загального фонду до території громади (тис. грн/км²). Даний показник показує, наскільки ефективно використовується такий ресурсу громади, як земля. Причому характеризує не лише отримання податкового платежу від володіння чи використання безпосередньо як земельного ресурсу, а і можливість розташування на певних площах виробничих потужностей, розвиток підприємницької діяльності. Таким чином прослідковується прямий взаємозв'язок між площею території громади і потенційними доходами, які бюджет даної громади отримує від її використання;

- доходи загального фонду на одного мешканця (без урахування міжбюджетних трансфертів) (грн) свідчать про зміни у власних доходах місцевих бюджетів на одну особу, в яких найбільша доля належить податковим надходженням, дає змогу оцінити діючу податкоспроможність територій в розрахунку на одного мешканця, порівняти із середніми по Україні, визначати стратегічні шляхи пошуку резервів податкових доходів громад і здійснювати горизонтальне вирівнювання податкоспроможності задля збалансованого розвитку територій і фінансової підтримки слабких в сенсі економічного розвитку регіонів.

- підприємницький потенціал, або співвідношення надходжень єдиного податку до числа мешканців відповідної територіальної громади (грн./ 1-го. мешканця

громади). Даний показник характеризує стан підприємницької активності, сприятливість умов на відповідній території для ведення бізнесу, наявність платоспроможного попиту на ту продукцію чи послуги, що реалізуються суб'єктами підприємницької діяльності та фізичними особами-підприємцями, які працюють на спрощеній системі обліку, оподаткування та звітності.

Отже, використання застосовуваних раніше і наразі введених методів оцінки податкового потенціалу сприятиме більш реалістичному прогнозуванню, плануванню доходів місцевих бюджетів із використанням резервних можливостей, і відповідно, адекватному фінансовому забезпеченню територіальних громад власними бюджетними коштами.

2. Аналіз податкового потенціалу формування доходів місцевих бюджетів в Україні.

Аналіз реалізованого складника податкового потенціалу здійснюємо на основі фактичних даних по надходженням податків і зборів до місцевих бюджетів України на основі офіційної звітності (<https://decentralization.ua/finance/dashboard>; Державний веб-портал бюджету для громадян URL: <https://openbudget.gov.ua>; Офіційний веб-сайт Міністерства фінансів України. URL: <https://minfin.com.ua>).

Спочатку доцільно проаналізувати місце податкових надходжень в обсязі всіх доходів місцевих бюджетів (МБ) і в загальній сумі податкових надходжень до зведеного бюджету України (ЗБ) (табл. 2.1, рис. 2.1, 2.2).

Таблиця 2.1

Динаміка і частка податкових доходів місцевих бюджетів України (МБ) протягом 2021-2023 рр.

Види доходів	2021	2022	2023	Відхил. відн, 2023/2021, %
1	3	4	5	5
Доходи МБ без МБТ	377965,9	418343,3	475223,9	25,7
Податкові доходи ДБ	1107090,9	949764,4	1203544,1	8,7
Податкові доходи МБ	346713,2	393460,6	434540,9	25,3
Всього податкові доходи ЗБ	1453804,1	1343225,0	1638085,0	12,7
Частка податкових доходів у доходах МБ, %	91,7	94,0	91,4	-0,3
Частка податків МБ у податкових доходах ЗБ, %	23,8	29,3	26,5	+2,7
Частка податків ДБ у податкових доходах ЗБ, %	76,2	70,7	73,5	-2,7

Джерело: побудовано за даними (<https://openbudget.gov.ua>)

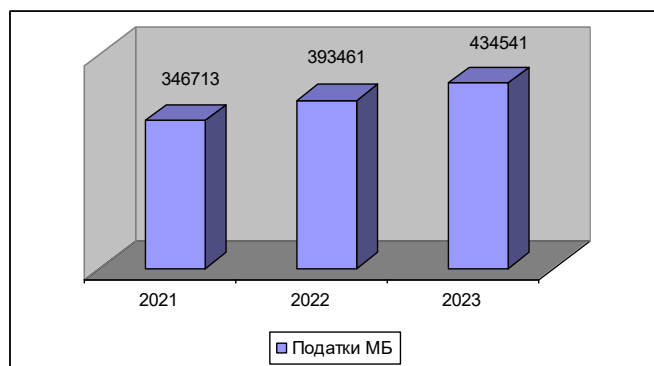


Рис.2.1 Динаміка податкових доходів місцевих бюджетів України, млн. грн
Джерело: побудовано за даними (<https://openbudget.gov.ua>)

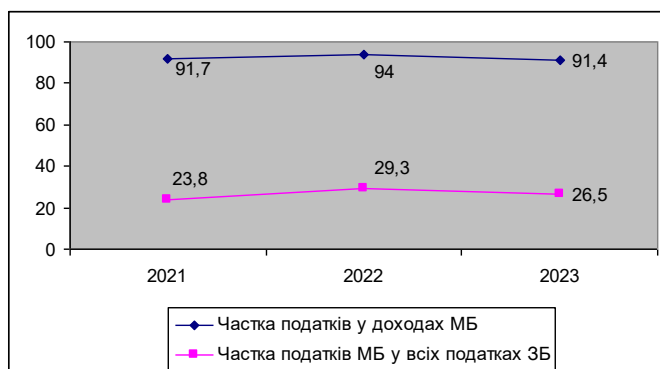


Рис.2.2 Зміна частки податкових надходжень місцевих бюджетів України за 2021-2023 рр.

Джерело: побудовано за даними (<https://openbudget.gov.ua>)

Як видно з табл.2.1, рис.2.1,2.2. суми фактичних податкових надходжень, що формують реалізовану частину податкового потенціалу, займають найбільшу питому вагу серед усіх видів бюджетних доходів. В динаміці спостерігається зростання як всіх доходів місцевих бюджетів (з трансфертами і без них), так і податкових доходів, а також податкових доходів державного бюджету України. Однак варто відзначити, що темп приросту податкових доходів місцевих бюджетів (25,3%) значно випереджає за аналізований період темп приросту обсягів податкових надходжень до державного бюджету України (8,7%).

Податки і збори у складі доходів місцевих бюджетів без міжбюджетних трансфертів традиційно займають більше 90%, що підкреслює їх значимість у формуванні фінансової бази органів місцевого самоврядування і забезпечення виконання ними їх функцій. Через деякі законодавчі зміни, а також мобілізацію зусиль на місцях частка податкових доходів і всіх податкових надходженнях зведеного бюджету зросла з 23,8% до 26,5% , що є позитивним моментом з огляду на процеси фінансової децентралізації.

Далі проаналізуємо склад, динаміку і структуру податкових доходів місцевих бюджетів у розрізі найбільш значимих (табл.2.2 , рис. 2.3).

Таблиця 2.2

Динаміка основних податкових надходжень до місцевих бюджетів України за 2021-2023 рр., млрд. грн

Види податків і зборів	2021	2022	2023	Відхил. відн, 2023/2021, %
ПДФО	212,2	272,3	289,4	36,4
Єдиний податок	46,3	47,2	55,8	20,5
Податок на майно	43,2	36,8	43,8	1,4
Податок на прибуток	16,1	13,5	15,5	-3,8
Акциз	17,8	13,1	22,4	25,8
Екологічний податок	2,1	1,6	1,3	-39,0
Інші (рента, туристичний, паркування)	9,0	9,0	6,3	-30,0
Всього	346,7	393,5	434,5	+25,3

Джерело: побудовано за даними (<https://openbudget.gov.ua>)

Аналіз динаміки податків свідчить про позитивну тенденцію по найбільш вагомим їх видах: ПДФО, податку на майно, єдиному та акцизному податках. По податку на прибуток, екологічному та інших податках і зборах спостерігаємо спадну тенденцію, обумовлену впливом воєнного стану.

Таблиця 2.3

Структура основних податкових надходжень до місцевих бюджетів України за 2021-2023 рр., млрд. грн

Види податків і зборів	2021	2022	2023	Відхил. абс, 2023/2021, %
ПДФО	61,2	69,2	66,6	5,4
Єдиний податок	13,4	12,0	12,8	-0,6
Податок на майно	12,5	9,4	10,1	-2,4
Податок на прибуток	4,6	3,4	3,6	-1,0
Акциз	5,1	3,3	5,1	-
Екологічний податок	0,6	0,4	0,3	-0,3
Інші (екологічний, рента, туристичний, паркування)	2,6	2,1	1,8	-0,8
Всього	100	100	100	-

Джерело: побудовано за даними (<https://openbudget.gov.ua>)

Унаочнення структури податкових надходжень до місцевих бюджетів України у 2023 р. наведено на рис.2.4.

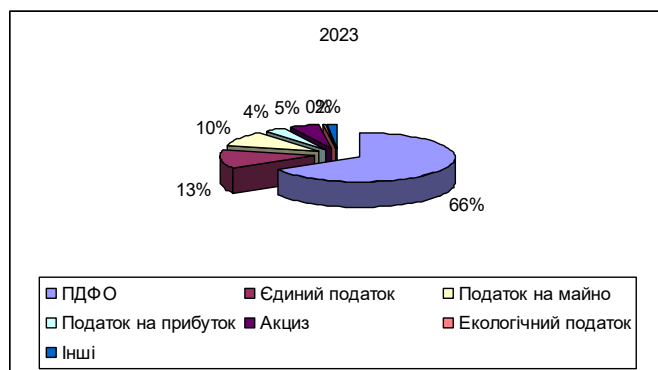


Рис.2.4 Структура податкових надходжень до місцевих бюджетів України у 2023 р.

Джерело: побудовано за даними (<https://openbudget.gov.ua>)

Найбільшим бюджетоутворюючим податком для місцевих бюджетів є податок з доходів фізичних осіб (приблизно дві третини податкових надходжень), який і структурно збільшився у 2023 році порівняно з 2021 р. Однак частка ПДФО скоротилась порівняно з 2022 р., коли питома вага його була 69,9%, що пояснюється вилученням з 01.10. 2023 р. до державного бюджету військового ПДФО, а також законодавчим поверненням до розподілу на користь місцевих бюджетів 60% від загальної суми ПДФО (а не 64%, як було в 2022 р).

Обсяг податку на прибуток скоротився через зниження / припинення економічної діяльності суб'єктів господарювання через воєнні дії на території країни.

Акцизний податок на пальне і на продаж збільшився за аналізований період на 25,8%, що є позитивним фактором для місцевих бюджетів. В абсолютних сумах і по структурі серед податкових надходжень виділяються єдиний податок і податок на майно (ПнМ), які належать до місцевих податків і зборів (МПЗ).

Оскільки місцеве оподаткування лежить в основі формування власної доходної бази, від якої залежить не тільки фінансування соціально-економічної сфери, виробничої інфраструктури, а і взагалі розвитку територіальних громад, тому детальніше проаналізуємо саме реалізовану складову потенціалу місцевих податків і зборів усіх місцевих бюджетів України (табл.2.4, рис.2.5).

Як свідчить аналіз, хоча в цілому місцеві податки і збори зросли на 11,1% у 2023 р. порівняно з 2021 р. завдяки суттєвому збільшенню сум єдиного податку і податку на нерухомість, однак в структурі всіх податкових надходжень зменшилися на 7%, це пояснюється більш прискореним зростанням у складі податкових доходів загальнодержавного ПДФО.

Таблиця 2.4

Склад і динаміка місцевих податків і зборів місцевих бюджетів України за 2021-2023 рр., тис. грн.

Види МПЗ	2021	2022	2023	Відхил. Відн. 2023/2021, %
Плата за землю	35 263,6	29 568,4	34 528,9	-2,1
Податок на нерухоме майно, відмінне від земельної ділянки	7 820,8	7 118,9	9 140,0	16,9

Транспортний податок	158,4	103,5	160,5	1,3
Єдиний податок	46 282,4	47 226,1	55 805,4	20,6
Туристичний збір	244,0	186,4	222,6	
Збір за паркування транспортних засобів	254,1	101,8	151,4	-8,8
Всього місцевих податків і зборів	90 023,3	84 305,1	100 008,8	11,1
Частка МПЗ у всіх податкових надходженнях МБ, %	30,0	21,4	23,0	-24,0

Джерело: побудовано за даними (<https://openbudget.gov.ua>)

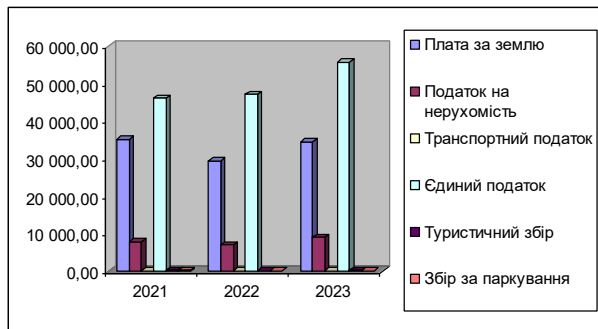


Рис.2.5 Динаміка МПЗ у місцевих бюджетах України, тис грн

Джерело: побудовано за даними (<https://openbudget.gov.ua>)

У структурі місцевого оподаткування в Україні превалюють плата за землю (зі спадною тенденцією через війну) та єдиний податок з позитивною динамікою через останні законодавчі зміни (разом більше 80%). Обсяги податку на нерухомість збільшилися на 16,9%, але досить вагомій ролі він поки що не відіграє у системі доходів місцевих бюджетів (табл. 2.5).

Таблиця 2.5

Структура місцевих податків і зборів в місцевих бюджетах України, %

Види місцевих податків і зборів	2021	2022	2023
Плата за землю	39,2	35,1	34,5
Податок на нерухоме майно, відмінне від земельної ділянки	8,7	8,4	9,1
Транспортний податок	0,1	0,1	0,1
Єдиний податок	51,40	56,0	55,9
Туристичний збір	0,3	0,2	0,2
Збір за паркування транспортних засобів	0,3	0,2	0,2
Всього місцевих податків і зборів	100	100	100

Джерело: розраховано за даними [<https://openbudget.gov.ua>]

Зниження надходжень плати за землю пояснюється зменшенням бази оподаткування через воєнні дії, недосконалою методикою оцінки земельних ресурсів і встановлення ставок, неефективним адмініструванням даного податку тощо. Тому тут є резерви збільшення реалізованої складової податкового потенціалу.

Інші місцеві податки і збори є порівняно незначними та складають не більше 1 % від усієї суми місцевого оподаткування. Протягом останніх років частка МПЗ не досягає 2 % від ВВП, а частка ПнМ менше 1 % у структурі ВВП, що надзвичайно обмежує виконання повноважень органами місцевого самоврядування щодо залучення і використання додаткових бюджетних ресурсів на фінансове забезпечення громад.

Для більш повного аналізу реалізованої складової податкового потенціалу доцільно обчислити показники податкового потенціалу формування доходів місцевих бюджетів. Оскільки деякі потрібні для аналізу показники у зв'язку із воєнним станом не оприлюднюються, скористаємося наявними офіційними даними щодо показника фіскальної віддачі території по окремих територіальних громадах (ТГ). (Дашборд «Бюджети територіальних громад України». URL: <https://decentralization.ua/finance/dashboard>). Для порівняння із більше ніж 1100 громад в Україні в таблиці 2.6 -2.8 наведено показники по громадах-лідерах, а також для порівняння у великих і значимих громадах Полтавської області.

Таблиця 2. 6

Показники фіскальної віддачі території деяких громад України у 2021 році

Місце в порядку рейтингу	Назва громади, область	Фіскальна віддача, тис.грн.
1 місце в рейтингу	Першотравенська, Дніпропетровська обл.	59644
2 місце в рейтингу	Одеська, Одеська обл.	56984
3 місце в рейтингу	Вишнева, Київська обл.	43548
24 місце в рейтингу	Кременчуцька, Полтавська обл.	12748
45 місце в рейтингу	Полтавська, Полтавська обл.	5760

Таблиця 2.7

Показники фіскальної віддачі території деяких громад України у 2022 році

Місце в порядку рейтингу	Назва громади, область	Фіскальна віддача, тис.грн.
1 місце в рейтингу	Одеська, Одеська обл.	60347
2 місце в рейтингу	Першотравенська, Дніпропетровська обл.	60250
3 місце в рейтингу	Вишнева, Київська обл.	58694
22 місце в рейтингу	Кременчуцька, Полтавська обл.	17187
45 місце в рейтингу	Полтавська, Полтавська обл.	7267

Таблиця 2.8

Показники фіскальної віддачі території деяких громад України у 2023 році

Місце в порядку рейтингу	Назва громади, область	Фіскальна віддача, тис.грн.
1 місце в рейтингу	Вишнева, Київська обл.	86437
2 місце в рейтингу	Одеська, Одеська обл.	66878
3 місце в рейтингу	Першотравенська, Дніпропетровська обл.	65114
19 місце в рейтингу	Кременчуцька, Полтавська обл..	19306
44 місце в рейтингу	Полтавська, Полтавська обл.	7490

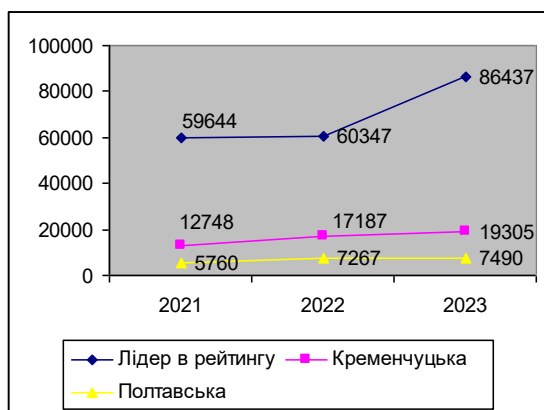


Рис. 2.6 Фіскальна віддача територій окремих ТГ в Україні протягом 2021-2023 рр., тис грн

Джерело: побудовано на основі (Дашборд «Бюджету територіальних громад України»). URL: <https://decentralization.ua/finance/dashboard>

Як видно з аналізу, трійка лідерів протягом аналізованого періоду була сталою. На рис.2.6 видно, що найвищі показники зросли в динаміці в 1.44 рази за 2021-2023 рр., по Кременчуцькій міській територіальній громаді фіскальна віддача території збільшилася в 1,51 рази, а по Полтавській міській територіальній громаді – в 1,3 рази.

Отже, реалізована складова податкового потенціалу формування доходів місцевих бюджетів є динамічною, відповідає змінам в законодавчому полі, економічному та політичному житті, зазнає впливу різних зовнішніх і внутрішніх факторів, які необхідно враховувати в процесі її вдосконалення.

Нереалізована складова податкового потенціалу спричиняє втрати доходів місцевих бюджетів через податкові розриви (тобто різниці між плановими і фактичними надходженнями), недоотримання податкових платежів в результаті існування податкового боргу, податкових пільг (податкових видатків), ухилення платників від сплати податків, а також втрати податкових надходжень через існування тіньової економіки.

Визначимо спочатку втрати доходів місцевих бюджетів України внаслідок тіньової економіки (табл.2.9).

Таблиця 2. 9

Втрати податкових надходжень від тіньової економіки

	2021	2022	2023
ВВП, млрд грн	5459,6	5191,0	6537,8
Рівень перерозподілу доходів МБ через ВВП, %	10,6	10,7	10,0
ВВП в розподілі доходів МБ млрд грн	549,6	555,4	653,8
Інтегральний показник рівня тіньової економіки, %	32	32	40
Потенційний рівень ВВП, млрд грн	725,5	733,1	849,9
Податкові надходження місцевих бюджетів, млрд грн	346,7	393,4	434,5
Бюджетний податковий коефіцієнт, %	63,0	70,8	66,5
Потенційні податкові надходження, млрд грн	457,1	513,2	564,8
Податкові втрати МБ від тіньової економіки, млрд грн	110,4	119,8	130,3

Джерело: розраховано автором за даними [Державний веб-портал бюджету для громадян]. URL: <https://openbudget.gov.ua>; офіційний веб-сайт Міністерства фінансів України. URL: <https://minfin.com.ua>].

Як видно з табл. 2.9, податкові втрати від тіньової економіки для доходів місцевих бюджетів за 2021-2023 рр. зросли на 18%, або на 19,9 млрд грн. Звісно, тіньова економіка знижує фінансовий потенціал місцевих органів влади, є засобом ухилення від сплати податків, чому треба активно протидіяти.

Таким чином, податкові втрати від тіньової економіки для місцевих бюджетів щороку протягом аналізованого періоду становлять майже третину від їх фактичних податкових надходжень.

Завдані в результаті тінізації економіки збитки покриваються коштами платників, які сумлінно виконують і перевиконують свої податкові зобов'язання. Однак варто враховувати, що рівень податкового навантаження має бути не дуже обтяжливим, щоб платники податків не лише розвивали свій бізнес, а й інвестували у розвиток територіальних громад. Тому особливо актуально виважено підходити до врегулювання податкових ставок, адже це стимулює ділову активність та зростання конкурентоспроможності вітчизняних підприємств і організацій, а в кінцевому підсумку сприяє зростанню податкових доходів до місцевих бюджетів.

Наступна складова нереалізованої частини податкового потенціалу пов'язана з несплатою суб'єктами оподаткування розрахованого податкового зобов'язання, яке утворює податковий борг. Податковий борг розглядається як фінансовий наслідок невиконання або неякісного виконання платниками обов'язкових платежів до місцевих бюджетів. На жаль, наявність системної статистики щодо податкового боргу в цілому, в розрізі державного і місцевих бюджетів, а також конкретних податків і зборів є проблематичною наразі. Тому в нашій роботі для аналізу використаємо доступні дані. Проаналізуємо за 2021-2023 рр. державний борг місцевих бюджетів України по найбільших податкових надходженнях: ПДФО і єдиному податку. Динаміку обсягів такої заборгованості відображено в табл. 2.10.

Таблиця 2.10

Динаміка податкового боргу місцевих бюджетів України за 2021-2023 рр., млрд. грн

Види боргу по податках	2021	2022	2023	Відхилення абс., +/-
Борг з ПДФО	4,2	4,61	12,02	+7,82
Борг з єдиного податку	2,03	4,0	3,51	+1,48
Всього борг до МБ по основних податках	6,03	4,0	15,53	+9,5

Джерело: побудовано за даними (<https://tax.gov.ua/diynalnist-/plani-ta-zviti-roboti-/791153.html>)

В динаміці сума податкового боргу зросла у 2,5 рази за аналізований період і становила у 2023 р. 15,53 млрд грн., або 3,5% від усіх податкових надходжень місцевих бюджетів, що є значним резервом їх доходної бази.

Проаналізуємо також наступний елемент нереалізованої складової податкового потенціалу - податкові пільги. Згідно з ПКУ, податкова пільга надається через:

встановлення зниженої ставки податку, звільнення від сплати податку, зменшення бази оподаткування, надання відстрочки і розстрочки платежів.

Податкове законодавство щодо пільгового оподаткування, а саме обліку, звітності щодо втрат бюджету від надання податкових преференцій, недосконале. Тому поряд з позитивними наслідками пільг прослідковуються і негативні їх ознаки, які виявляються в їхній необ'єктивності і неефективності щодо суб'єктів, об'єктів, що веде до провокування на ухилення від оподаткування.

Через обмеження сучасної інформаційної бази щодо надання податкових пільг і втрат доходів бюджету всього, в тому числі по місцевих бюджетах, аналіз проведено за попередній період (рис.2.8). Як видно з рис.2.8, обсяги пільг, що ведуть до втрат податкових доходів місцевих бюджетів України постійно зростали. За аналізований період збільшилися в 2,5 рази і у 2019 р. втрати місцевих бюджетів становили 9,24 млрд грн., серед них найбільше – по податку на майно.

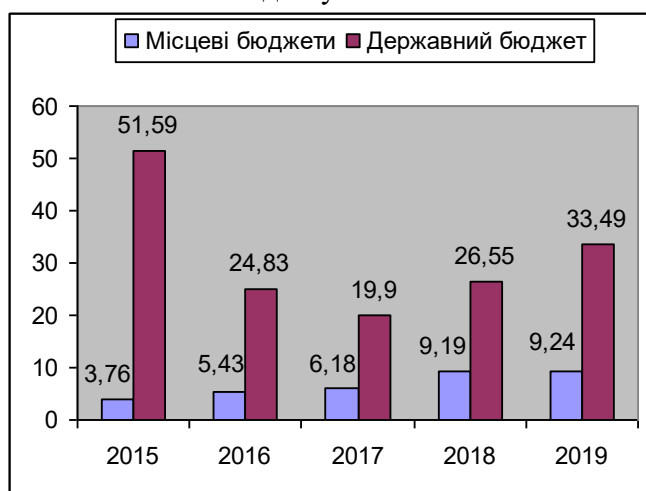


Рис.2.8 Розподіл втрат бюджетів від надання податкових пільг, млрд. грн.

Джерело: побудовано за даними (Марчак Д., Маркуц Ю., 2020)

В період повномасштабної війни з РФ кількість податкових пільг звісно, обсяги їх значно зросли (по майновому податку, єдиному податку, ПДФО та інших).

Податкові пільги, маючи на меті реалізацію регулюючої функції, стимулювання платників до інвестицій, але водночас при нераціональному їх застосуванні завдають збитків державі, адже ведуть до втрат доходів як місцевих бюджетів, так і державного.

Звичайно, в Україні певні заходи щодо вдосконалення пільгового оподаткування здійснюються (наприклад, обмеження галузевих пільг, введення обліку податкових пільг на підприємствах, деяке покращення податкового адміністрування, скорочення кількості пільг по окремих податках), однак ефективність таких заходів залишається поки що низькою.

Отже, є суттєвий вплив на втрати доходів бюджету від застосування податкових пільг, наявності податкового боргу.

Узагальнимо обсяг втрат місцевих бюджетів від нереалізованої складової податкового потенціалу за 2021-2023 рр. (табл. 2.11).

Таблиця 2.11

Втрати від нереалізованої складової податкового потенціалу України (2021-2023рр.)

Показники	2021	2022	2023
Податковий розрив від тіньової економіки, млрд. грн.	110,4	119,8	130,3
Питома вага, %	94,8	96,8	89,4
Загальна сума податкового боргу, млрд. грн.	6,03	4,0	15,53
Питома вага, %	5,2	3,2	10,6
Всього, млрд. грн.	116,43	123,8	145,83

Джерело: розраховано автором

Як видно з табл. 2.11, основним джерелом податкових втрат є тіньова економіка.

Отже, розраховані втрати місцевих бюджетів України від нереалізованої складової податкового потенціалу протягом 2021-2023 рр. зросли на 25,3%, і склали в 2023 р. 145,83 млрд грн., що становить 33% від фактично отриманих податкових надходжень у цьому році до місцевих бюджетів, а це є значним резервом зростання доходної бази бюджетів.

3. Напрями вдосконалення інструментарію реалізації податкового потенціалу формування доходів місцевих бюджетів.

Серед усіх джерел наповнення реалізованої складової податкового потенціалу доходів місцевих бюджетів України особливо виділяються наразі ПДФО, акцизний податок і місцеві податки (єдиний податок, плата за землю і трохи менше - податок на нерухоме майно. Обсяги податкових надходжень визначають бази оподаткування конкретних податків, ставки, механізм обчислення і сплати, законодавче врегулювання та ефективність адміністрування податкових платежів.

Розглянемо потенціал зростання ПДФО у складі місцевих бюджетів.

Інтенсивне зростання фактичного надходження ПДФО у 2022 р. зумовлено збільшенням відрахувань із заробітних плат військовослужбовців і збільшенням нормативу зарахування до місцевих бюджетів до 64% з 60% . Однак з 1 жовтня 2023 року ПДФО з військових було вилучено з місцевих бюджетів, що негативно вплинуло на приріст в подальшому цього загальнодержавного податку.

В Україні в даний час використовується пропорційна система оподаткування ПДФО, передбачено застосування податкової соціальної пільги в межах граничних розмірів заробітної плати. З підвищенням мінімальної заробітної плати, яка перевищила граничну зарплату для отримання пільги, частина працюючих громадян втратила право на її отримання, а це порушує принцип соціальної справедливості, підвищується податковий тягар для менш заможних, що є проблематичним в діючому механізмі оподаткування ПДФО.

Для вирішення цієї проблеми доцільно повернутися до прогресивної системи оподаткування яка діяла уже в Україні і взагалі вважається більш справедливою, оскільки передбачає застосування вищих ставок податку до вищих доходів, причому на цьому наголошують як науковці, практики, так і законодавці.

У Національній стратегії доходів України до 2030 року в якості реформування

прибуткового оподаткування доходів громадян оголошено перехід до прогресивної від пропорційної із запровадженням підвищених ставок ПДФО, але без деталізації диференціації таких ставок. Передбачається, що застосування підвищених ставок, Наприклад, на рівні 25% і 35% потенційно принесло б у 2022 р. 32 млрд грн., що становить 8% додатково доходів ПДФО (*Національна стратегія доходів: аналіз впливу на органи місцевого самоврядування*. URL: <https://decentralization.ua/news/17374?page=0>).

Також в Національній стратегії пропонується скасування соціальної податкової пільги - неоподаткованого мінімуму доходів громадян, замінивши її цільовою допомогою для соціально незахищених працюючих громадян. Така пропозиція є прийнятною на період повномасштабної війни для більшої акумуляції в доходах ПДФО, але потім варто повернутися до податкової соціальної пільги (URL: <https://decentralization.ua/news/17374?page=0>).

Проблематичним наразі залишається і розподіл платників за рівнем доходу та обґрунтування кількості ставок їх впливу на збільшення доходів.

Звичайно, на мобілізацію коштів ПДФО також суттєвий вплив мають кількість працівників та обсяг ухилення від оподаткування. Тому актуальним залишається боротьба з неофіційним працевлаштуванням, виплатою зарплати «у конвертах». Заходи з легалізації оподатковуваних доходів громадян проводяться відповідними органами, але потрібне більше оприлюднення результатів контрольних заходів і їх реалізації.

Правильне обчислення планових сум ПДФО, ретельний аналіз впливу факторів на обсяги податку, застосування методів економіко-математичного моделювання при прогнозуванні й плануванні даного податку з урахуванням можливих ризиків, а також використання цифрових технологій в процесі податкового адміністрування – це важливі передумови ефективної реалізації податкового потенціалу ПДФО (реалізована складова).

Важливою проблемою щодо ПДФО як джерела доходів місцевих бюджетів є те, що сума цього податку надходить до бюджету за місцем роботи працюючих, а не за місцем їх проживання в територіальних громадах., фінансове забезпечення яких за рахунок ПДФО стає обмеженим, а працюючі громадяни не сповна отримують соціальні послуги за місцем свого проживання. Для вирішення даної проблеми потрібно удосконалити порядок розподілення податку з доходів фізичних осіб між бюджетами таких територіальних громад.

Невдовзі до Бюджетного та Податкового кодексів України мають внести зміни стосовно зарахування податку за місцезнаходженням підприємств, а не за місцем реєстрації юридичних осіб. Це сприятиме удосконаленню механізму горизонтального вирівнювання місцевих бюджетів, наданню стимулів в ОМС для місцевого економічного розвитку, збільшенню власних доходів.

Для розвитку фінансової самостійності місцевого самоврядування, нарощування доходної бази місцевих бюджетів важливу роль відіграють місцеві податки і збори. Для порівняння і оцінки податкового потенціалу порівняємо місцеві податки на одного мешканця в розрізі видів територіальних громад (таблиця 3.1).

Таблиця 3.1

Динаміка місцевих податків і зборів в розрахунку на 1 мешканця

	Середня сума надходжень місцевих податків і зборів, в розрахунку на 1 мешканця, грн/особу		
	2021	2022	2023
Міські ТГ	1 708,3	1 570,5	1 864,6
Із них Кременчуцька МТГ	1792,5	1737,5	2137,2
Селищні ТГ	1 909,2	1 674,9	2 177,9
Сільські ТГ	2 190,4	2 041,2	2 530,6
Середнє значення по ТГ України	1 978,1	1 806,2	2 248,2

Джерело: побудовано на основі (Дашборд «Бюджети територіальних громад України». URL: <https://decentralization.ua/finance/dashboard>)

Як видно з аналізу табл.3.1, за період 2021-2023 рр. зростання надходжень місцевих податків і зборів залежить від типу територіальних громад: найменше зростання було по міських громадах – 9,2%; по селищних і сільських збільшення відповідно - 14,1% і 15,5%.

Характерно, що і розмір місцевих податків і зборів на 1 мешканця в міських громадах менше, ніж у громадах іншого типу. Причиною таких тенденцій надходжень місцевих податків на одного мешканця є те, що в сільських громадах через недостатність або відсутність надходжень від загальнодержавних податків більше уваги приділяють мобілізації саме місцевих податків і зборів.

У структурі місцевих податків найбільшу частку займає єдиний податок, який сплачують суб'єкти, що працюють на спрощеній системі оподаткування (ССО). Зростання ролі ССО пояснюється в сучасних умовах головним чином доступністю та привабливістю даного пільгового режиму в порівнянні зі звичайною системою оподаткування, а також можливістю досягнення меншого податкового навантаження.

Реформування даної системи спрямоване на збільшення фіскальної віддачі і передбачає:

- поступове протягом наступних трьох років збільшення ставки єдиного податку для юридичних осіб 3-ої групи до 18 %, як і для оподаткування прибутку для звичайної системи оподаткування;

- об'єднання другої та третьої групи для фізичних осіб-підприємців в одну другу, суб'єкти якої будуть сплачувати податок від доходу на основі диференційованої шкали ставок, причому теж із поступовим збільшенням та інші.

В структурі місцевого оподаткування потенційно високий дохід, як свідчить досвід зарубіжних країн, має майновий податок. В Україні один із найбільших майнових податків – плата за землю, по якій спостерігаємо значне зменшення частки – із 44,6% у 2019 році до 34,5% у 2023 (*Державний веб-портал бюджету для громадян*. URL: <https://openbudget.gov.ua>). Обсяг плати за землю до місцевих бюджетів впливає на розмір і динаміку показника «дохідність земель громади». Динаміка показника плати за землю є в основному спадною через широкомасштабну війну рф і визначається різними значеннями в залежності від самих громад.

Проблемами у оподаткуванні плати за землю є відсутність ефективного та дієвого механізму впровадження та застосування економічно обгрунтованої для

цілей оподаткування оцінки землі, недостатньо і неповністю проведена інвентаризація використовуваних земель, встановлення якісних і кількісних їх характеристик, в результаті чого база оподаткування є неповною, а це – резерв реальних надходжень плати за землю у складі майнового податку.

Окрім недонадходження плати за землю через окупацію територій, бойові дії та руйнації, засмічення земель, зниження економічної активності бізнесу, міграцію населення, на зниження податкового потенціалу доходів місцевих бюджетів від плати за землю вплинули і пільги, які запроваджені були через воєнний стан.

Великий потенціал зростання бюджетних доходів криється в одному із місцевих податків і зборів – податку на нерухоме майно, відмінне від земельної ділянки, частка якого у їх структурі доходів місцевих бюджетів України зросла з 6,6 % в 2021 р. до 9,1% в 2023 р. Ця тенденція свідчить про необхідність вдосконалення механізму справляння даного податку з урахуванням позитивного світового досвіду для підвищення рівня фінансової спроможності та стійкості територіальних громад.

Податок на майно у більшості країн світу є однією з головних статей доходів місцевих бюджетів. Але на відміну від України, де цей податок розраховується на основі площі об'єкта нерухомості, в світовій практиці при розрахунку податку обчислюють і використовують вартість нерухомості (наприклад, кадастрову в Італії, Іспанії, ринкову вартість – у США).

Кадастрова вартість – це ціна нерухомості, що встановлюється на базі оцінки або в результаті незалежної експертизи і вноситься до бази, яка формується на державному рівні. Оподаткування об'єктів нерухомого майна у різних країнах, переваги і недоліки кожної із систем різні.

В Україні, звичайно, перевагою використання площі об'єкта нерухомості як бази оподаткування є відносна простота адміністрування, але вона не відображає зносу, вартості поліпшень, місця розташування та інших важливих характеристик майна. Однак більшість нерухомого майна фізичних осіб під оподаткування не потрапляє, адже податком обкладаються: квартири, площа яких більше 60 м² і будинки – перевищення площі 120 м². Ставки податку визначає місцева влада, але її розмір повинен бути в межах 1,5 % мінімальної заробітної плати. На жаль, сьогодні відсутня повна база об'єктів оподаткування. До Державного реєстру прав на нерухоме майно значну частину об'єктів нерухомості не внесено, тому і база оподаткування значно занижена.

В національній Стратегії доходів до 2030 року в контексті збільшення доходів місцевих бюджетів за рахунок податку на нерухомість пропонується удосконалення здійснення оцінки майна, об'єктів нерухомості, що містяться в Державному реєстрі майнових прав на нерухомість, запровадження оподаткування нерухомості, виходячи з оціночної вартості, наповнення інформаційної бази даними щодо оціночної вартості об'єктів.

На нашу думку, це сприятиме реальному наповненню реєстрів, збільшенню надходжень податку за рахунок бази оподаткування і в цілому – зростанню бюджетних ресурсів територіальних громад.

Також необхідною є чітка взаємодія податкових органів і органів місцевого самоврядування щодо адміністрування даного податку, яка має бути регламентована у відповідних офіційних документах.

Звичайно, при удосконаленні процесу справляння податку на нерухомість потрібно створити ефективні методики оцінювання вартості майна, чіткі нормативи, за якими можна здійснювати оцінку стану та реальної та ринкової вартості нерухомого майна, що оподатковується. Також необхідне проведення суцільної інвентаризації нерухомого майна, відмінного від земельної ділянки. Відповідно, що це тривалий процес, тому нову модель оподаткування податком на нерухоме майно планується розробити у 2027-2028 роках (<https://decentralization.ua/news/17374?page=0>).

Реальна складова податкового потенціалу залежить у значній мірі від адміністрування податків і зборів, зокрема місцевих. Органи місцевого самоврядування не мають наразі повноважень стосовно адміністрування податків і зборів. Податковий кодекс визначає, що податкові органи повинні давати місцевим органам повну і детальну інформацію стосовно нарахування та сплати платежів на території громади. Однак часто ця норма не дотримується, що негативно впливає на планування та виконання доходів їхніх бюджетів.

В Нацстратегії доходів до 2030 року щодо реформи адміністрування місцевих податків та зборів планується здійснення заходів:

- підготовка змін в законодавство щодо надання органам місцевого самоврядування додаткових повноважень в частині адміністрування місцевих податків і зборів, особливо податку на нерухоме майно;
- проведення органами місцевого самоврядування інвентаризації земельних ділянок, об'єктів нерухомості, відображення реальної інформації у відповідних державних реєстрах;
- законодавчо закріпити права ОМС щодо доступу до інформаційних баз податкової служби відносно місцевих податків і зборів, в тому числі, їх втратах у доходах в результаті пільгового оподаткування тощо.

Отже, обсяги реалізованого податкового потенціалу доходів місцевих бюджетів залежать від багатьох чинників зовнішніх і внутрішніх, врахування яких в ході бюджетного менеджменту на місцевому рівні сприятиме нарощуванню доходної бази бюджетів місцевого самоврядування для повного, своєчасного фінансового забезпечення місцевих територіальних громад та якісного виконання ними власних і делегованих повноважень.

Нереалізований податковий потенціал формування доходів місцевих бюджетів є значним резервом збільшення таких доходів, формування фінансово спроможної громади. Основні інструменти уникнення податків в Україні схожі і до інших країн. До них, зокрема, відносять: інструменти тіньової економіки (тіньові заробітні плати, тіньовий ринок землі, неофіційне підприємництво тощо), відтік доходів в офшори, викривлення бази оподаткування, легальна мінімізація податкових зобов'язань та інші.

Розглянемо деякі з цих інструментів, як вони впливають на стан формування податкових доходів місцевого бюджету.

Тіньова оренда сільськогосподарських земель пов'язана з тим, що багато років більшість землі сільськогосподарського призначення обробляли на умовах оренди, а велика частка орендних договорів належним чином не реєструвалася, відповідно, від

орендодавців ПДФО не сплачувався, що призводило до недоотримання податкових доходів.

Через неофіційну зайнятість і заплати у конвертах умовні втрати бюджетних надходжень і єдиного соціального внеску, за розрахунками, становлять від 115 до 230 млрд грн. (Черкашин В., Саварець А, 2023). Відсутність статистичних даних щодо неформальної зайнятості, кількості найманих працівників у роки повномасштабної війни не дають можливості здійснити більш реально оцінку обсягів схем потенційних втрат доходів бюджету, тому боротьба за легалізацію заробітної плати є важливим кроком для потенційного зростання ПДФО, єдиного податку.

Ухилення від сплати податків за допомогою спрощеної системи оподаткування – 3 групи ФОП здійснюється задля мінімізації оподаткування податком на прибуток і реалізується шляхом подрібнення великих підприємств на псевдо-ФОП, які сплачують єдиний податок. В результаті недоотримані бюджетні надходження наприклад, у 2023р. становили біля 1 млрд грн (Черкашин В., Саварець А, 2023).

Зміни до законодавства, війна, економічна криза та інші чинники призвели до зростання обсягів зловживань за певними схемами, які потрібно виявляти й мінімізувати. Узагальнення порівняльного аналізу фіскального ефекту за 2023 р. від схем ухилення та уникнення оподаткування для місцевих бюджетів подано в таблиці 3.2.

Таблиця 3.2

Порівняльний аналіз фіскального ефекту від схем ухилення/уникнення оподаткування для місцевих бюджетів

Схема	Податки (платежі), яких вона дає змогу уникати	Приблизні втрати бюджету, млрд. грн
Схеми з оподаткуванням землі та нерухомості	ПДФО, податок на прибуток	18-20
Заробітні плати в конвертах	ПДФО	115-230
ССО – ФОП замість найму 3 група	ПДФО	4–10

Джерело: складено автором на основі (В. Дубровський, О.Гетман, В.Черкашин,2024)

Отже, приблизні втрати доходів місцевих бюджетів вражаючи від ухилення/уникнення від оподаткування через застосування різних схем, але вони є податковим нереалізованим потенціалом.

Податкові пільги є нереалізованим податковим потенціалом, якщо вони надаються безсистемно, без аналізу їх результативності, впливу на соціально-економічний розвиток.

На жаль, в Україні, хоч публікують офіційно довідники податкових пільг. однак звітність по них не оприлюднюють, а така непрозорість веде до марних податкових видатків, нераціонального формування бюджетних ресурсів.

У сучасних умовах для більш ефективного впливу пільгового оподаткування доцільно:

- додати до Податкового кодексу України розділ «Податкові пільги», в якому визначити загальний порядок встановлення, зміни та скасування податкових пільг,

напрямки їх використання, ведення обліку, здійснення контролю за цільовим використанням коштів, вивільнених у зв'язку з пільговим оподаткуванням;

- об'єктивно і компетентно, з урахуванням аналізу впливу на доходи бюджету, переглянути існуючі види пільг щодо податків і зборів на законодавчому рівні;
- впроваджувати зарубіжну практику складання податковими органами щорічних звітів про податкові видатки бюджету та їх оприлюднювати.

Важливо зазначити, що Міністерство фінансів України розробило та затвердило у вересні 2024 року Методологію проведення оцінювання інструментів податкової політики, які призводять до податкових видатків (*Наказ Міністерства фінансів України 27 вересня 2024 року № 474, 2024*).

Оцінка податкових пільг дозволить визначити їх дієвість і більш ефективно використовувати обмежені бюджетні кошти, що особливо важливо в умовах воєнного стану. Причому передбачається систематичне прогнозне оцінювання на етапі бюджетного планування та ретроспективне оцінювання для визначення ефективності застосування податкових пільг.

Для вдосконалення управління податковим боргом доцільно:

- впроваджувати IT-рішення для контролю податкового боргу в розрізі платників податків, бюджетів, видів податкових надходжень;
- спростити процедури розстрочення та відстрочення податкових зобов'язань для фізичних і юридичних осіб;
- посилити взаємодію щодо зменшення/ліквідації податкового боргу фінансових і податкових органів;
- залучати органи місцевого самоврядування до контролю за податковим боргом і збільшенням завдяки цьому доходів місцевого бюджету.

Визначення можливостей здійснення нереалізованої складової податкового потенціалу формування доходів місцевого бюджету разом з його реалізованою складовою дає змогу при діючих умовах оподаткування прогнозно оцінити обсяг податкових надходжень (реальних і потенційних).

Оцінка податкового потенціалу може стати основою удосконалення визначення податкоспроможності території. На нашу думку, доцільно при визначенні податкоспроможності територіальної громади використовувати не тільки ПДФО (за діючою методикою), а й плату за землю і єдиний податок, які є вагомою складовою реалізованого податкового потенціалу, формують фінансову доходну базу місцевих бюджетів. Тобто податкоспроможність на одного мешканця громади пропонується визначати за такою формулою:

Податкоспроможність = (ПДФО + Єдиний податок + плата за землю) / число мешканців територіальної громади.

Аналогічно показник можна розраховувати і по всіх територіальних громадах України.

За нарощування податкового потенціалу в динаміці (виражається як темп росту) за такими джерелами як скорочення податкового боргу, податкових розривів щодо виконання плану пропонуємо окремим територіальним громадам або зменшувати розраховану реверсну дотацію або збільшувати базову дотацію. Таке коригування міжбюджетних трансфертів за використання потенційних можливостей зростання

доходів стимулюватиме зацікавленість ОМС в усіх регіонах до економічного розвитку, обґрунтованого збільшення бюджетних ресурсів територіальних громад в процесі горизонтального вирівнювання.

Звичайно, розрахунки стануть більш складними, але в умовах діджиталізації цілком реальні. Варто зазначити про можливість використання методів математичної статистики при визначенні прогнозної складової податкового потенціалу при плануванні доходів місцевого бюджету.

Таким чином, визначення податкового потенціалу доходів місцевих бюджетів в абсолютних величинах сприятиме більш повному і обґрунтованому формуванню бюджетних ресурсів за рахунок податкових надходжень в окремо взятих територіальних громадах.

Індекс податкового потенціалу доходів як відносний показник дає змогу здійснювати порівняльний аналіз між відповідними показниками різних громад і середнім по Україні з метою виявлення сильних і слабких у розвитку податкового потенціалу регіонів, відповідно удосконалення фінансового вирівнювання і кращого забезпечення необхідними фінансовими ресурсами територій.

Висновки. На сучасному етапі соціально-економічного розвитку територіальних громад, коли їх фінансове забезпечення бюджетними ресурсами надзвичайно ускладнено через кризові явища, воєнний стан, основними пріоритетами формування ефективної фінансової політики на регіональному рівні є виявлення і використання резервів економічного зростання, активізація наявних фінансових механізмів та інструментів розвитку, зокрема комплексна оцінка податкового потенціалу регіону та розробка напрямів його нарощування й використання прихованих доходних джерел місцевих бюджетів.

Податковий потенціал є найважливішою складовою бюджетної системи кожної держави, виступає фундаментом формування її податкових доходів. Саме здатність органів місцевого самоврядування трансформувати податкову базу бюджетної системи на місцевому рівні в податкові доходи фактично дає їм можливість реалізовувати свої функції, зокрема впливати на господарські процеси в суспільстві. Ефективність реалізації податкового потенціалу місцевого самоврядування здійснює безпосередній вплив на рівень соціально-економічного розвитку окремих територій.

Встановлено, що за своїм змістом податковий потенціал – це прогнозний обсяг податків і зборів до місцевих бюджетів, який сформований задля максимально можливого наповнення бюджетів територіальних громад фінансовими ресурсами з урахуванням мінімально можливих втрат податкових доходів, в тому числі за рахунок недоотримання потенційних податків через податкові пільги, податковий борг, ухилення від оподаткування.

В роботі визначено та досліджені основні складові податкового потенціалу: реалізована, нереалізована та прогнозована.

Реалізована складова відображає мобілізацію фактичних податкових надходжень до місцевих бюджетів. Проведений аналіз показав, що податкові надходження є основним бюджетоутворюючим джерелом доходів як державного, так і місцевих бюджетів. Виявлені основні проблеми формування податкового потенціалу в його реалізованій складовій. Доведено необхідність виваженого підходу до реформування ПДФО, плати за землю, єдиного та податку на нерухомість, від

мобілізації яких залежить в основному фактична мобілізація обсягів податкових доходів у місцевому бюджеті.

Водночас, в ході дослідження виявлено значні обсяги податкових втрат, що формує нереалізована складова податкового потенціалу, а саме: надання податкових пільг, існування податкового боргу, загрозливий рівень тіньової економіки, що проявляється в результаті ухилення та уникнення сплати податків і зборів.

Прогнозована складова податкового потенціалу передбачає можливості збільшення його розмірів за рахунок економічного зростання внаслідок розширення видів діяльності, кардинальних змін в системі оподаткування, підвищення якості прогнозування й бюджетного планування доходів місцевих бюджетів на основі комплексної оцінки всього податкового потенціалу громад, економіко-математичного моделювання, використання всіх можливостей діджиталізації в бюджетній і податковій сферах на регіональному рівні.

Обсяги всіх складових податкового потенціалу доходів місцевих бюджетів залежать від багатьох чинників зовнішніх і внутрішніх, врахування яких в ході бюджетного менеджменту на місцевому рівні сприятиме нарощуванню доходної бази бюджетів місцевого самоврядування для повного, своєчасного фінансового забезпечення місцевих територіальних громад та якісного виконання ними власних і делегованих повноважень. Також ефективна реалізація функціонування цих складових податкового потенціалу дозволить не тільки протистояти правопорушенням у податковій сфері, збільшивши податкові доходи місцевих бюджетів, а й підвищить фінансову спроможність і стійкість територіальних громад та їх місцевих бюджетів.

References:

- Буряченко А. Економічна природа фінансового потенціалу регіону. *Наукові записки Національного університету «Острозька академія». Серія «Економіка» : науковий журнал*. Острог : Вид-во НУ «ОА». 2016. № 3(31). С. 96–102. URL: <https://ecj.oa.edu.ua/articles/2017/31/20.pdf>
- Бюджетний кодекс України: Закон України від 08.07.2010 р. № 2456– VI. URL: <http://zakon0.rada.gov.ua/laws/show/2456-17>.
- «Дашборд «Бюджети територіальних громад України». URL: <https://decentralization.ua/finance/dashboard>.
- Державний веб-портал бюджету для громадян. URL: <https://openbudget.gov.ua>
- Дубровський В., Гетман О., Черкашин В. Порівняльний аналіз фіскального ефекту від застосування інструментів ухилення/уникнення оподаткування в Україні. Київ, 2024. Інститут соціально-економічної трансформації. URL: <https://surl.li/pbzgwf>
- Каламбет С. Податковий потенціал у механізмі регулювання економічного зростання: автореф. дис. на здобуття наук. ступеня канд. екон. наук . Донецьк, 2003. 32 с. URL: <file:///D:/Downloads/AREF.DOC.pdf>
- Канева Т. В., Рубан М. О. Оцінювання податкового потенціалу адміністративно-територіальної одиниці. *Проблеми економіки*. Вип. № 3 (37), 2018. С.191-200. <https://surl.li/bgarjo>
- Канева Т., Карпенко М. Методологічні засади формування доходної частини місцевих бюджетів за сучасних умов. *Економіка та суспільство*. 2024. (59). <https://doi.org/10.32782/2524-0072/2024-59-55>
- Методологія проведення оцінювання інструментів податкової політики, які призводять до податкових видатків. Наказ Міністерства фінансів України 27 вересня 2024 року № 474. URL: <https://surl.li/iyemdp>

- Марчак Д., Маркуц Ю. Невидимі субсидії. Хто і скільки втрачає, а хто — отримує в Україні від податкових пільг? URL: <https://surl.li/zzpsoi> (дата звернення 21.02.2025).
- Міщенко Д. А., Перетятко А. В. Податковий потенціал як основна складова бюджетних можливостей регіону. *Ефективна економіка*. 2017. № 12. URL: <http://www.economy.nayka.com.ua/?op=1&z=5924>
- Національна стратегія доходів»: аналіз впливу на органи місцевого самоврядування. URL: <https://decentralization.ua/news/17374?page=0>
- Олексій М.Ф. Податковий потенціал регіону: проблеми та перспективи розвитку. Науковий вісник Ужгородського університету. Серія «Економіка». 2024. Випуск 1(63). 112-115 УДК 336.22. DOI: <https://doi.org/10.24144/2409-6857.2024.1>
- Офіційний вебпортал Кременчуцької міської ради Кременчуцького району Полтавської області та виконавчого комітету. URL: <https://kremen.gov.ua/?view=city&page-id=83>
- Офіційний веб-сайт Міністерства фінансів України. URL: <https://minfin.com.ua>
- Педченко Н.С. Податковий потенціал як основна складова бюджетних можливостей регіону (на прикладі Полтавської області). *Сталий розвиток економіки*. 2011. №4(7). С. 298–304. URL: <http://dspace.puet.edu.ua/handle/123456789/1009>
- Податковий кодекс України від 02.12.2010 № 2755-VI URL: <https://zakon.rada.gov.ua/laws/show/2755-17#Text>
- Публічний звіт ДПС України за 2023 рік. URL: <https://surl.cc/wtaxgd>
- Сідельникова Л., Боровік Л., Осадча, Т. Вектори впливу системи оподаткування на розвиток підприємницької діяльності в Україні. *Цифрова економіка та економічна безпека*, (6 (15), 377-383. <https://doi.org/10.32782/dees.15-60>
- Тарангул Л.Л. Податкова політика та економічний розвиток регіонів: теорія, методологія, практика: дис. на здобуття наук. ступеня д-ра екон. наук: спец. 08.04.01/ НАН України ; Ін-т екон. прогнозування. К., 2003. 379 с. URL: <file:///D:/Downloads/DISERTACIYA.doc.pdf>
- Тенденції тіньової економіки. Міністерство економіки України. URL: <https://surl.li/lsmigt>
- Цимбалюк І., Антонюк Д., Карлін М. Проблематика оцінки податкового потенціалу регіону як іманентної складової фіскального простору. *Економіка та суспільство*. Випуск № 39 / 2022. DOI: <https://doi.org/10.32782/2524-0072/2022-39-18>
- Цимбалюк І. О., Редько І. М. Формування та оцінка податкового потенціалу регіонів України. Економічний вісник університету: збірник наукових праць учених та аспірантів. Переяслав-Хмельницький : Державний вищий навчальний заклад «Переяслав-Хмельницький державний педагогічний університет імені Григорія Сковороди», 2013. Вип. 20/2. С. 216–221. URL: <https://core.ac.uk/download/pdf/153578402.pdf>
- Черкасова О. С. Податковий потенціал регіону: сутність та методика оцінки. *Сталий розвиток економіки*. 2014. № 3. С. 138–143. URL: http://nbuv.gov.ua/UJRN/sre_2014_3_24
- Черкашин В., Саварець А. Моніторинг ефективності Державної податкової служби та Державної митної служби. Інститут соціально-економічної трансформації. Київ. URL: Monitoring-DPS-DMS-2023-final1.pdf

CHAPTER 11. DIGITALIZATION OF PUBLIC AUTHORITY SERVICES AND THE PUBLIC SECTOR OF UKRAINE: STATE, TECHNOLOGIES, AND CHALLENGES

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 paper analyzes the state of digitization of public authorities and the public sector of Ukraine, in particular in the context of the initiative "State in a Smartphone". The development of digital infrastructure, in particular the Diia platform, which enables citizens to access more than 30 administrative services and store 21 types of digital documents, is studied. The development of electronic interaction between government agencies through the Trembita system and other pivotal components of the digital infrastructure is considered. Examples of the implementation of digital tools in healthcare, education, anti-corruption and the financial sector are discussed. The paper highlights the main challenges and risks of implementing the considered innovative digital tools. Possible measures to overcome these problems are suggested.

Keywords: digitalization, digital transformation, Diia, e-government, infrastructure, information technology.

Introduction. The development of information technology contributes to the global digital transformation that encompasses all spheres of society, including public administration. Ukraine is actively implementing the concept of a digital state, which involves the extensive use of electronic technologies to provide public services and ensure effective interaction between citizens and the government. One of the key areas of this transformation is the "State in a Smartphone" initiative, launched in 2019 by President Zelenskyy. This initiative aims at the transition of all government services to an online format and is actively implemented by the Ministry of Digital Transformation of Ukraine and other state institutions.

The effectiveness of digitalization processes is confirmed by a significant increase in position of Ukraine in international rankings.

One of the most important achievements of digital transformation was the creation of the national platform "Diia" for electronic interaction between the state and citizens. This platform allows users to receive more than 30 types of administrative services, store 21 types of digital documents, and perform various legally significant operations. Today, 20.9 million Ukrainians use this platform, which greatly simplifies access to government services. By 2024, it was planned to transfer 100% of government services to "Diia".

The development of a digital state in Ukraine is based on the best international

practices, in particular on the experience of Estonia, which has become a world leader in e-governance. Estonia was the first country in the world to introduce electronic interaction of registries and ID cards, online voting, and to achieve a 99% online service rate. The adoption of innovative technologies such as electronic identification, digital document management, and electronic registries enhances the efficiency of public administration while reducing bureaucracy and corruption.

At the same time extensive digital transformation of the state is associated with various problems and challenges.

The purpose of this study is to analyze the state of digitalization of public authorities and the public sector in Ukraine, identify key challenges and risks, and suggest possible solutions to overcome them.

Research methods include systematic analysis, comparative research, and generalization of international practices in the field of e-government.

Analysis of the overall state of digitalization of public authorities and the public sector in Ukraine

The **E-Government Development Index (EGDI)** is a comprehensive index developed by the United Nations to assess the readiness of countries to use information and communication technologies (ICT) to deliver public services.

Ukraine		E-Government (2024 EGDI: 0.8841)	
Website	National Portal	2024 Rank	30
Region	Europe	Group	VHEGDI
Sub-Region	Eastern Europe	Rating Class	V3
Income *	Lower middle income	2022 Rank	46
Income Value	2,388 USD, GNI per capita	Change	-16
Population	44,657,704	E-Participation (2024 EPART: 1.0000)	
E-Government Development Index	0.8841 Rank 30 of 193	2024 Rank	1
E-Participation Index	1.0000 Rank 1 of 193	2022 Rank	57
		Change	-56

* Income data refer to World Bank classification

According to the EGDI 2024 study presented on the United Nations Public Administration Network platform, Ukraine's EGDI has been growing in absolute value in recent years, indicating progress in the development of e-government in the country.

According to the EGDI, the country has risen from 46th to 30th place among 193 countries over the past two years, which indicates significant progress in the field of digital services compared to other countries:

Table 1. Dynamics of rank and value of E-Government Development Index in Ukraine

E-Government Development Index	2024	2022	2020	2018	2016	2014	2012	2010	2008	2005	2004	2003
Ukraine (Rank)	30	46	69	82	62	87	68	54	41	48	45	54
Ukraine (Value)	0.88407	0.80290	0.71190	0.61650	0.60756	0.50316	0.56530	0.51808	0.57280	0.54561	0.53255	0.46167

EGDI is a weighted average of the three indices. The main components of the EGDI are Online Service Index, Telecommunication Infrastructure Index, and Human Capital Index.

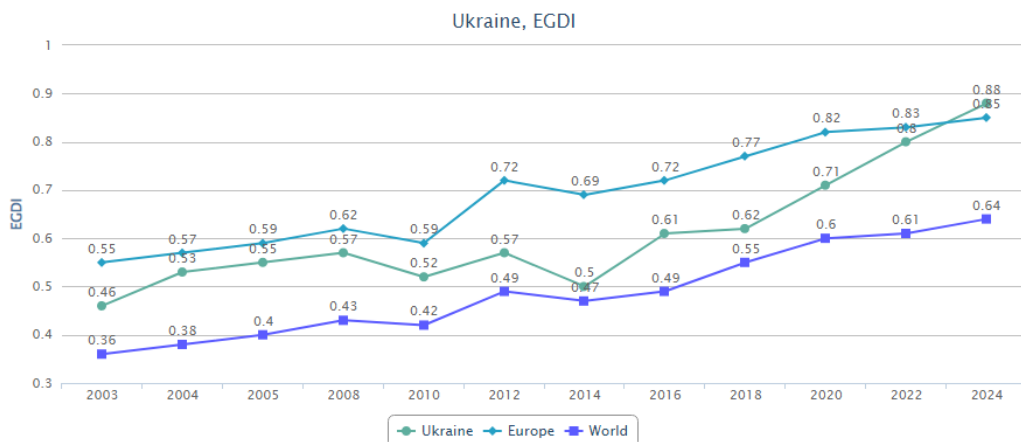


Fig. 1. Dynamics of E-Government Development Index

Source: <https://surl.li/qeoxun>

Online Service Index (OSI) is a metric that measures the scope and quality of online services provided by national governments. It includes aspects such as information provision, citizen participation and transactional services. According to the Online Service Index, Ukraine has risen from 32nd to 5th place in the world in two years, thereby demonstrating a high level of development of e-government services.

Table 2. Dynamics of Online Service Index in Ukraine

Online Service Index	2024	2022	2020	2018	2016	2014	2012	2010	2008	2005	2004	2003
Ukraine (Value)	0.98536	0.81480	0.68240	0.56940	0.58696	0.26771	0.42483	0.34603	0.53511	0.58076	0.55598	0.34934

Telecommunication Infrastructure Index (TII) is a metric that analyzes the development of a country's telecommunications infrastructure, which is necessary for citizens to access e-government services. According to the TII, Ukraine ranks 78th in the world. However, the dynamics of the TII shows a steady increase in the index.

Table 3. Dynamics of Telecommunication Infrastructure Index in Ukraine

Telecommunication Infrastructure Index	2024	2022	2020	2018	2016	2014	2012	2010	2008	2005	2004	2003
Ukraine (Value)	0.84278	0.72700	0.59420	0.43640	0.39677	0.38016	0.35349	0.24869	0.23357	0.11607	0.11166	0.11568

Human Capital Index (HCI) is a metric that measures the ability of citizens to use electronic government services, including the level of literacy and education of the population. According to the HCI, Ukraine ranks 47th in the world with a stable trend in the index.

Table 4. Dynamics of Human Capital Index in Ukraine

Human Capital Index	2024	2022	2020	2018	2016	2014	2012	2010	2008	2005	2004	2003
Ukraine (Value)	0.82402	0.86690	0.85910	0.84360	0.83895	0.86160	0.91758	0.96473	0.95083	0.94000	0.93000	0.92000

Fig. 2 illustrates the dynamics of changes in the index and its components from 2003 to 2024.

Countries with low levels of human capital may face difficulties in implementing e-government. However, the results of a study on the digital skills of Ukrainians, conducted as part of the Diia.Education project at the initiative of the Ministry of Digital Transformation of Ukraine, show a steady increase in the level of digital skills of the population. This is reflected in decrease in the proportion of adults without digital skills and an increase in the population with basic and advanced skills.

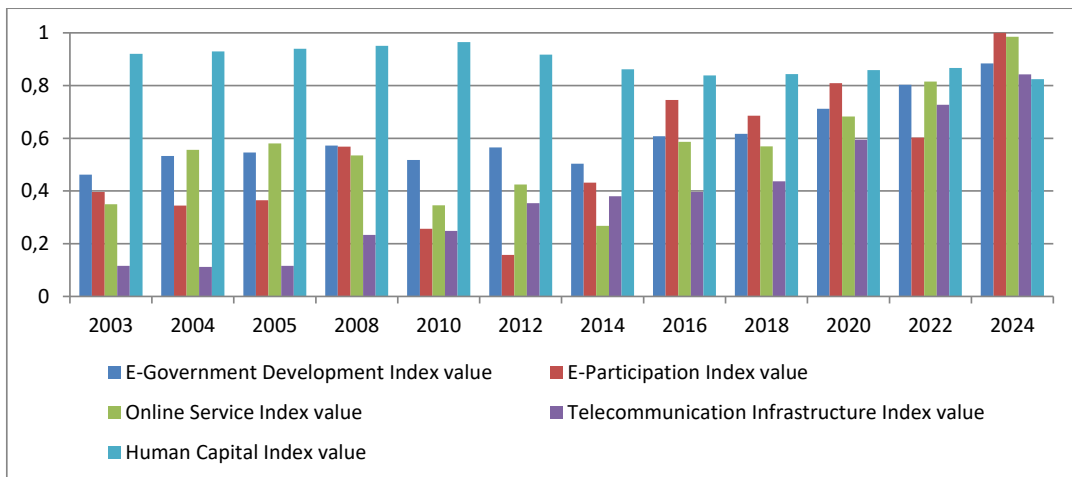


Fig. 2. Dynamics of E-Government Development Index

The survey of digital skills of Ukrainians has been conducted every two years since 2019. According to the first survey in 2019, 53% of Ukrainians had less than basic digital skills, and 47% of citizens expressed interest in learning. By 2023, however, the situation had improved significantly.

By 2023, digital skills were possessed by: 93% of Ukraine's adult population aged 18-70 (+8% compared to 2019); 95% of youth aged 10-17. 38% of the adult population had mastered advanced digital skills (+12.5% compared to 2019). The share of adults with less than basic digital skills decreased from 53% to 40.4% (a decrease of 12.6%).

Thus, the findings of the Digital Skills Survey of Ukrainians demonstrate the positive dynamics of digital literacy development in Ukraine, which contributes to the effective implementation of e-government.

In addition, Ukraine ranked first in the E-Participation index, which indicates the active involvement of citizens in government processes through online platforms.

Key component of Digital Government include (Fig. 3):

Key Components of Digital Government

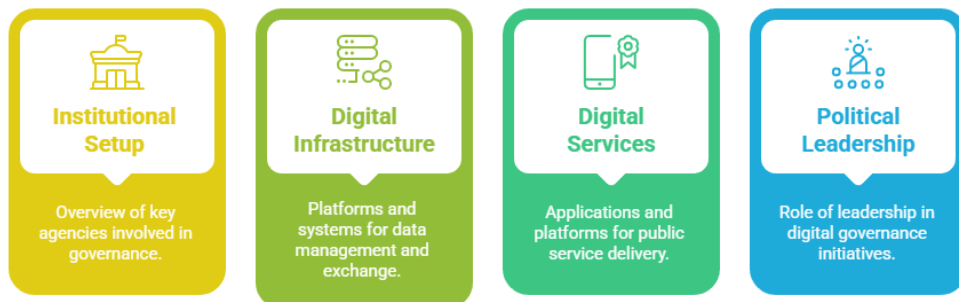


Fig. 3. Key component of Digital Government

1. Institutional Setup:

State Agency for e-Governance – Established in 2014, responsible for digital government policies.

Ministry for Digital Transformation – Created in 2019, oversees digital development.

2. Digital Infrastructure:

Trembita – Launched in 2018, government data exchange platform.
State Registry of Registries – Developed in 2018 to manage state registries.

3. Digital Services and Platforms

Diia App – Introduced in 2020, provides digital services.

Diia Education – A platform for reskilling and digital literacy.

Information Systems of State Sector – The systems for managing digital processes in the public sector.

4. Political Leadership and Crisis Response

Let's consider these elements in detail.

Development of Digital infrastructure of electronic document management systems

The “Trembita” system plays a pivotal role in Ukraine's digital infrastructure, facilitating the secure exchange of electronic data between government agencies and registries.

The “Trembita” system is a system of electronic interaction of state electronic information resources implemented within the international technical project EGOV4Ukraine based on the X-Road platform used in Estonia. It is being developed with the support of the European Union within the EU4DigitalUA and DT4UA projects. The “Trembita” is designed to ensure secure interagency cooperation through the exchange of electronic messages between the information systems of state and local governments. The system enables the transfer of data from various state registers in order to provide citizens with the necessary services.

The system includes web clients and web services for data exchange between information resources. The system is connected to 220 state and local government agencies, as well as 111 electronic information resources (EIRs). Over 340 electronic interactions between registers have been implemented.

Since the launch of the system in 2020, it has facilitated over 4 billion transactions. The majority of transactions take place between the Diia platform and the State Register of Individuals – Taxpayers. To ensure the effective functioning of the system, 17 indicators have been developed to monitor its status and the resources connected to it.

The Trembita system plays a pivotal role in ensuring the interoperability of Ukraine's state information systems and in supporting the Diia project.

Blinova N. (2021) has noted that the accounting of state electronic information resources faces a number of problems, in particular, the lack of systematization and classification enshrined in a regulatory act, which leads to the use of various concepts such as “portal”, “automated information system”, “information and communication system”, etc. Additionally, there is an absence of a comprehensive set of general principles and guidelines that would regulate the organization, functioning, use and storage of state electronic information resources.

Addressing these issues is crucial for the development of the country's digital infrastructure. A key element in the development of the country's digital infrastructure is the National Registry of Electronic Information Resources. Its implementation is aimed at systematization and classification of state electronic information resources, establishment of unified standards for their operation and preservation, as well as increasing transparency and efficiency of their management.

The National Registry of Electronic Information Resources (NREIR) is a state repository created to account for all electronic information resources of the state, including registers, cadastres, classifiers and information systems that ensure their functioning and use their information. The Registry ensures the registration, accounting, accumulation, processing and storage of information on the composition, content, location and conditions of access to electronic information resources.

The NREIR was established in accordance with the Resolution of the Cabinet of Ministers of Ukraine dated May 10, 2018, No. 357.

The NREIR plays an instrumental role in ensuring the interoperability of state information systems and providing support to the Trembita project, which aims to develop a decentralized system of information exchange between state registries.

The public service portal “Diia”, launched in 2020, has emerged as the brand of the digital state in Ukraine.

The Diia public service portal “Diia” is a pivotal component of digital transformation of Ukraine, which was initiated by the Ministry of Digital Transformation in 2020 as a component of the State in a Smartphone concept. It integrates a web portal, a mobile application, and the Diia.Osvita platform, thereby facilitating online access to administrative services for both citizens and businesses.

The portal provides more than 30 types of government services online and supports 21 types of digital documents, including passports, pension certificates, driver's licenses, and student ID cards. The functionality includes administrative services (e.g., formation of certificates, permits, change of residence), social services (e.g., applying for benefits, pensions, subsidies), business process automation (e.g., business registration, filing tax reports, access to state registers), and payment of fines and taxes. By 2024, more than 20.9 million people used the platform.

At the same time, the functioning of Diia is accompanied by several challenges. Technical challenges include necessity of large-scale infrastructure modernization and the risk of system overload with the growing number of transactions. Security threats stem from the centralized storage of data, which increases the vulnerability to cyberattacks and information leaks. Social aspect includes the problem of the digital gap of population and insufficient level of digital literacy. Finally, legal challenges are related to the lack of a unified legislative regulation of electronic services and the need to improve personal data protection regulations.

Consequently, the “Diia” portal is fundamentally changing the way citizens interact with the state, but its further development requires improving the technical infrastructure, strengthening cybersecurity, and improving the legal framework.

The Ukrainian model of digital democracy and the Diia app are attracting international attention. In May 2023, the Minister of Digital Transformation Fedorov M. presented it in the European Parliament, outlining Ukraine's digitalization strategy. During the Diia in DC summit in Washington, D.C., Diia was presented in the USA. It was noted that the development experience was shared between Colombia and Zambia. The growing interest of other countries in implementing similar solutions confirms the effectiveness of the Ukrainian approach.

In March 2024, it was announced that the Diia code base was made available in the Open-Source format on the GitHub platform, which will facilitate the international

dissemination of this technology.

Implementation of digital anti-corruption tools, ensuring effective functioning of the justice information system

The Unified Register of Pretrial Investigations (URPI) is an automated electronic database created to collect, store, protect, record, search and summarize data on criminal offenses and the course of pre-trial investigations in Ukraine. The Register was launched simultaneously with the entry into force of the Criminal Procedure Code of Ukraine on November 20, 2012. The main functions of the URPI are to provide a unified record of criminal offenses, operational control over the pre-trial investigations and analysis of the state of criminal offenses in Ukraine. The URPI contains data on criminal offenses, persons involved in criminal proceedings, as well as information on investigative actions and procedural decisions. The Register provides operational control over compliance with laws during the pre-trial investigation and analysis of the status and structure of criminal offenses in Ukraine. Access to the URPI is restricted and available only to law enforcement agencies and parties to criminal proceedings.

The issues related to the maintenance of the URPI and the information and telecommunication system were addressed by Lisnichenko D.V., Mudretska H.V., Kyslenko D.P., Stolychnyi A.V., Topchii N.S., Kalancha I.G., Popovych M.V. et al. The main risks are the problem of integration of registers and information systems of public authorities and cyberattacks on government and public resources.

In December 2024, the most significant external cyberattacks on Ukraine's state registries in recent times took place. As a result of the attack, the Unified and State Registers, which are under the jurisdiction of the Ministry of Justice of Ukraine, were temporarily suspended. According to Microsoft, published in its annual Digital Defense report for 2024, Russia, Iran and North Korea have changed their cyberattack tactics. In particular, they began experimenting with artificial intelligence.

In June 2023 (public part in August 2023), NACP launched the **Information System for Monitoring the Implementation of the State Anti-Corruption Policy**. This system provides key information on the results of the implementation of Ukraine's anti-corruption policy, including the status and dynamics of the implementation of state anti-corruption programs adopted for a certain period. The system currently provides the results of monitoring and evaluation of the implementation of the State Anti-Corruption Program for 2023-2025 and statistics on the work of specially authorized entities in the field of anti-corruption for 2023 and 2024.

The system allows executors to organize, plan and execute the State Anti-Corruption Program activities, and citizens and experts to track their progress. This increases the transparency of government activities.

The eCase Management System (eCMS) is an electronic system for the management of criminal proceedings developed for the anti-corruption agencies of Ukraine with the support of the EU Anti-Corruption Initiative (EUACI). In February 2022, the servers of the system were evacuated and the eCMS was suspended until August 2022. In August 2022, the National Bureau and the Specialized Anti-Corruption Prosecutor's Office returned to using the eCase Management System. Integration with the Unified Register of Pretrial Investigations (URPI) is implemented.

Use of the system faces a number of challenges. According to a report by the EU

Anti-Corruption Initiative (EUACI), the system is not fully utilized and is not used appropriately by individual users. The system does not currently provide access for defense counsel, as this feature is still under development. It is also not used by the Appeals Chamber of the HACC. Implementation is complicated by difficulties in staff adaptation, technical limitations and other obstacles to full use. Therefore, in order to analyze the state of system implementation, to assess the level of information security and integration with other digital platforms, in particular SMEREKA and Electronic Court, a tender was held to find specialists to review the implementation of eCase.

Digitalization of the public finance management system

The state prioritizes the digitalization of management processes at all levels of financial and budgetary management (Barych-Tinovska L.P., Durman O.L., 2022). Krynytsia S. (2024) has studied the features and analyzed the current strategies of digitalization of the public financial management system in Ukraine.

The digitalization of public authorities and e-government was considered by Klimushkin P. and Nesterenko O. Digitalization of the public finance management system was studied by Amaglobeli D., Amosov O., Atkinson E., Barr N., Hrytsenko L., Gupta S., Diaz N., Dubov D., Dunayev I., Efymenko O., Hrytsiak T., Kolomytseva A., Krantz O., Krynytsia S., Kud A., Long S., Mateus R., Matvienko H., Mengistu A., Movchanova N., Nose M., Simone E., Tantsi V., Janowski T., Vlasiuk O., Zhommot F., Zhuk I., Zakharkina L., Zakharkin O. et al. These issues are also the focus of research by influential international organizations at the international level, such as the World Bank, G-20, International Monetary Fund, World Economic Forum, UNCTAD, UN Commission for Social and Economic Development, etc.

In November 2021, the Cabinet of Ministers of Ukraine approved “Strategy for Digital Development, Digital Transformation and Digitalization of Public Financial Management System until 2025”. According to the strategy, the main approach is “the centralization of IT resources and IT functions of the Ministry of Finance and central executive bodies, whose activities are directed and coordinated by the Cabinet of Ministers of Ukraine through the Minister of Finance, with the priority use of cloud technologies, creation of a single data warehouse, gradual transition to a new level of service-oriented systems by ensuring the availability of public services online”. The strategy declares the goal “to build a modern and effective information technology management system with a view to ensuring the support and further digital development of an effective and transparent public finance management system”.

The document focuses on the automation and digitalization of processes. The transition to a paperless environment and electronic document management, the implementation of information systems for data processing and their exchange between different executive authorities, etc. are among the task top priorities.

In parallel with this strategy, “The strategy for public finance management system reform in 2022 – 2025” was adopted in November 2021. The section “Information Technology in Public Finance Management” is dedicated to digitalization.

The utilization of information technology in public finance management is aimed at achieving the overall strategic objective of enhancing transparency and accountability in public finance management.

As Krynytsia S. (2024) emphasizes, the digitalization strategy is a key component of the digital transformation of the public sector. The benefits mentioned include transparency,

more efficient use of funds and budgetary inclusion.

However, the public finance management system has a number of problems with the digitalization of public finances, in particular:

- Lack of integration among information systems within the public finance management framework;
- Lack of a centralized cloud data storage accessible to all state and local authorities;
- Outdated IT platforms used for automating public finance management processes;
- Limited automated in data exchange across different government levels;
- Limited internal workflows automation and high share of paper-based processes;
- Absence of unified methodology, standards, or approaches for designing IT platforms, complicating the effective integration of fragmented public finance management systems into a single system;
- Absence of a comprehensive information security system for certain public finance management IT platforms;
- Uncoordinated development of information systems of various central government agencies, resulting in redundant data flows and overlapping functionalities, etc.;
- Insufficient of qualified staffing for the maintenance and development of public finance management IT systems.

The primary measures to address these issues include the implementation of unified IT standards, the development of the Unified Information and Telecommunication System for Public Finance Management, the transition to electronic services, particularly the adoption of a user-oriented service model for the provision of IT services, the preservation and strengthening of human resources, and the protection of information processed in the Unified Information and Telecommunication System for Public Finance Management.

The utilization of digital technologies, such as artificial intelligence (Farooq Kh., Solowiej B.), machine learning (report of Organisation for Economic Co-operation and Development, 2024), big data analysis (Chekina V., Knyazev S., 2019, Vakshynska N., Shandrivska O., 2023, Collosa A, 2021, Gritsyak N., Tverdokhlib O. (2020), and smart contracts (Stankevych A., 2025, Kryvenko Yu., 2023, Serhiyenko O., Samus P., 2023, Nekit K., 2021, Ivanov A., Shmyha V., 2022), has been identified as a potential solution for enhancing the quality of work in budget and financial sectors. The active use of big data is confirmed by the fact that Ukraine ranks 25th in the Ranking: The Top 25 Countries with the Most Data Centers.

In financial sector, Smart contract is an agreement written in the form of computer code, which is executed automatically when certain conditions are met. Smart contracts operate based on blockchain technology and utilize cryptographic mechanisms to ensure data security and immutability. The key benefits and disadvantages of the smart contracts are presented in Fig. 1. One of the negative aspects of smart contracts is their immutability, which provides protection against unauthorized interference, but also makes it impossible to correct errors in the code after it is deployed. A notable illustration of this problem is the 2016 incident with The DAO project, described by Kryvenko Yu. (2023). In this instance a vulnerability in the wallet's smart contract code allowed attackers to repeatedly retrieve ETH before calculating the correct balance, resulting in the theft of 3.6 million ETH (equivalent to more than \$4.5 billion as of September 22, 2022). This case demonstrates the crucial need to develop mechanisms for secure updates.

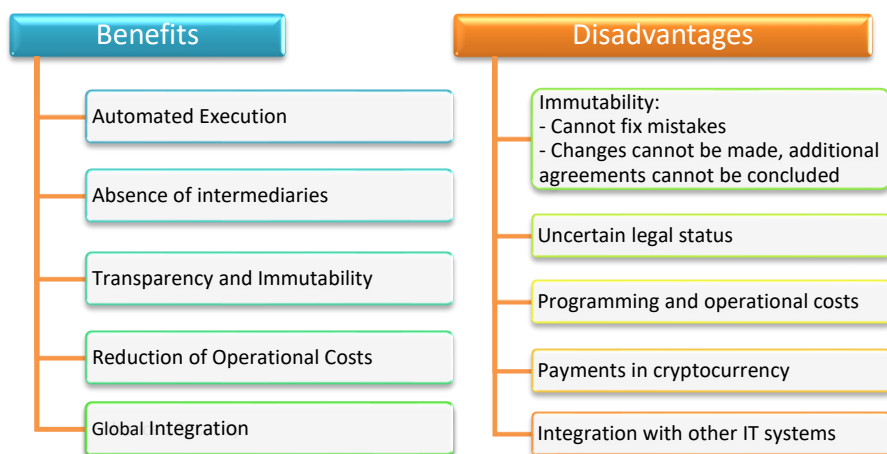


Fig. 4. Benefits and disadvantages of smart contracts in financial sector

Unified Web Portal of spending Public Funds (<https://spending.gov.ua/new/>) is an official state information resource on the Internet, where information on the use of public funds in Ukraine is published to ensure transparency of their movement. The portal was developed in accordance with the Law “On Openness of Public Funds Spending” and launched on September 15, 2015. The portal provides free access to information on transactions of the State Treasury Service, use of state and local budgets (since November 2015), as well as expenditures of state and municipal enterprises (since January 2016).

The portal contains the following information in tabular and graphical form: information on payment transactions on the Single Treasury Account, payments by state and municipal institutions, the Pension Fund of Ukraine and other state funds; information on contracts and status of their execution; reports and summary indicators.

In 2018-2020, a generalized information and analytical system “Transparent Budget” was created to inform the public about the financial and budgetary policies of Ukraine in an accessible form. The unified web portal is a part of the Transparent Budget IAS. This IAS creates opportunities for a transparent dialog between the government and the public on budget planning and execution at the state and local levels. The Transparent Budget IAS is actively used in research to analyze public finances, evaluate the effectiveness of budget programs and study corruption risks.

The Transparent Budget IAS unites three key modules of open data in the field of public finance and budgeting:

- Unified Web Portal of Spending of Public Funds (<https://Spending.gov.ua>) is the most extensive open database in Ukraine in the field of public finance. By March 28, 2025, the portal has already recorded about 253.2 million transactions (including UAH 854.7 billion for the current year) for UAH 29,183.5 billion (including 4.0 million for the current year).

- The Budget for Citizens (<https://Openbudget.gov.ua>) is the largest budget knowledge base, which contains key budget terms and deadlines of the budget process, indicators of the state and local budgets in the form of open data. The Budget for Citizens provides BOOST-analysis capabilities as part of the service.

The BOOST analysis (Budget Overview and Strategy Tool) is a unique tool developed

according to the World Bank methodology, which allows for the analysis of budgets at all levels: from community to state, in terms of revenues, expenditures, lending and financing. The goal is to use budget funds efficiently, improve decision-making processes, and assess transparency and accountability. BOOST analysis of the Budget for Citizens contributes to increasing the transparency and efficiency of public finances through the analysis of budget indicators at all levels by analysts and civic activists.

– The Register of Projects of International Financial Institutions (<https://proifi.gov.ua>) in Ukraine. It contains detailed information on social and economic development projects in Ukraine that are implemented partially or fully at the expense of concessional lending from international financial organizations (IFIs).

The system is also integrated with other government platforms. It allows citizens, researchers, and public authorities to access detailed information on budget expenditures, financial transactions, and use of public resources. Thus, the Transparent Budget IAS is a key element in ensuring transparency and accountability in the use of public funds, as well as an important resource for academic research in the field of public administration and finance.

Basiuk O. P. (2022) examines the World Bank's activities in financing projects around the world aimed at increasing transparency and openness in public finance, as well as the experience of using digital solutions to optimize the budget process in different countries, considers possibilities of financing for Ukraine as well.

Analogues of these systems in the world are the United States: USAspending.gov portal in the United States, which provides detailed information on federal spending, including contracts, grants and other financial transactions; Open Government Portal in Canada, which provides access to data on the use of public funds, including budget expenditures and financial statements; data.gouv.fr portal in France, which is a national open data portal and includes information on budget expenditures and financial transactions of the state; Portal Otwartych Danych (Open Data Portal) in Poland, which provides access to information on the use of public funds, including budget expenditures and financial statements.

Digitalization of education

In context of the global spread of COVID-19 and the transition of many services to digital or online format, the European Commission has developed the Digital Education Action Plan (2021-2027), which outlines the European Commission's vision for quality, inclusive and accessible digital education in Europe.

At the current stage of society's development, digital transformation and the transition to Education 4.0 are taking place.

Education 4.0 is a concept that reflects the transformation of education in context of the Fourth Industrial Revolution (Industry 4.0). It focuses on flexible, personalized learning that integrates modern digital technologies and prepares students to work in conditions of automation, artificial intelligence, and rapid changes in the technological environment.

The Ministry of Education and Science of Ukraine has developed “Education 4.0: Ukrainian Sunrise” (2022) program as part of the Ukraine's Post-Victory Recovery Plan. It provides for the education system's compliance with the technological principles of Industry 4.0 and digitalization in education (implementation of modern digital educational infrastructure, development of digital content for educators, and launch of a digital educational passport in a smartphone).

DIGITAL TRANSFORMATION OF EDUCATION AND SCIENCE

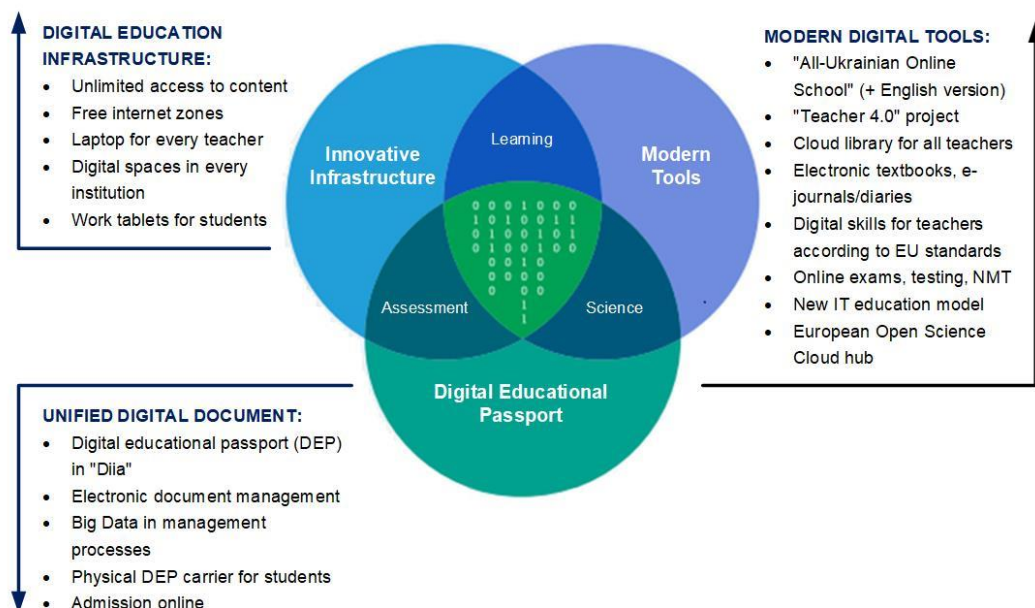


Fig. 5. Digital Transformation of Education and Science

Source: <https://mon.gov.ua>

According to the concept of Education 4.0, Ukraine is implementing the strategic plan of the Ministry of Education and Science of Ukraine until 2027, "Education of Winners" (2024). According to these programs, the priority of the Ukrainian education system is to increase the level of digital literacy among students and teachers, and to provide educational institutions with modern information and communication tools and technologies.

Bokhonko E., Shelever O., Dereka K. (2023) have identified the following categories of information and communication technologies within Education 4.0:

- technologies (artificial intelligence and machine learning, data processing using Data Science, data analytics and cloud computing, as well as virtual image processing for virtual and learning environments);

- tools and platforms (synchronous online sessions to support student learning using web conferencing technologies (ZOOM, Meets, Webex, M-Teams) and asynchronous learning platforms (LMS).

The main challenges in implementing the concept of Education 4.0 are the high demands on infrastructure and the lag of institutional changes in higher education institutions from the growth of technological innovations.

The issues of digitalization of education are addressed in the works of V. Bykov, A. Gurzhiy, M. Zhaldak, M. Leshchenko, N. Morse, O. Ovcharuk, Y. Ramsky, O. Spivakovsky, O. Spirin; K. Ala-Mutka, H. Albaqami, D. Belshaw, G. Creeber, L. Eutsler, A. Hernández, J. Hernández-Ramos, C. Huilcapi-Collantes, T. Koval, N. Maiier, G. Reynolds, J. Stommel et al.

Malytska I. (2023) has considered the issue of developing digital literacy of teachers during a period of martial law. The paper provides an overview of educational platforms

(Global Skills Academy, Global Teacher Campus and Global Learning House) and educational resources (from COURSERA, ProFuturo, Microsoft, etc.) to improve digital literacy. Special attention is paid to the support of UNESCO. The author noted that the UNESCO Global Education Coalition supports the Ukrainian educational community on an ongoing basis.

Malykhin O. et al (2024) has studied the digitalization of specialized secondary education, considered the benefits and challenges of digitalization of education, and raised the issue of the content of digital competencies of a modern teacher. According to their research, a modern teacher should have digital competencies that include:

- Integration of ICT in education: psychological and pedagogical principles, digital transformation, didactic potential of technologies.
- The use of universal digital tools as a means of communication, organization of the educational process, learning and assessment:
 - The need to systematize digital resources: the rapid development of ICT requires constant updating and monitoring of effective learning tools.
 - Motivation and self-development of teachers: the successful implementation of technologies depends on the willingness of teachers to learn and adapt.

The issue of digital transformation of Ukrainian education was discussed at the Reporting Scientific Conference of the Institute of Digitalization of Education of the National Academy of Pedagogical Sciences of Ukraine “Digital Transformation of Ukrainian Education under Martial Law”, held on February 24, 2023. The reports of the conference participants identified modern trends in the development of digital technologies for open education and science, described the theoretical and practical aspects of design and use modern learning tools in a computer-oriented environment, in particular, use of cloud and immersive technologies.

The Ministry of Digital Transformation of Ukraine, with the support of the Swiss-Ukrainian EGAP Program, implemented by the Eastern Europe Foundation and funded by Switzerland, conducts a study to assess the level of digital skills of Ukrainians Every two years since 2019. The third wave of the study aims to track the dynamics in the development of digital skills of the Ukrainian population and analyze the impact of the socio-economic situation on the level of digital security. The basis for determining the level of digital skills is the European Commission's methodology for calculating the Digital Economy and Society Index, namely the Digital Skills Indicator [2017 methodology], which is based on the Digital Competence Framework. The results are available at <https://osvita.diia.gov.ua/research>.

In order to increase the level of digital literacy of the population of Ukraine, the Ministry of Digital Transformation of Ukraine launched the **Diia.Osvita** project as part of the Diia initiative.

Diia.Osvita is an educational project aimed at developing digital education and increasing the level of digital literacy among the population of Ukraine in such areas as working with data, programming, and using digital tools through access to quality digital education (Mokliak V., Bondarenko T., 2023). The project offers educational programs and courses in such areas as programming, data analysis, cybersecurity, and other digital technologies for various age groups and professional levels, as well as opportunities to build an individual learning path. Education is provided through online platforms with interactive

tools, which ensures access to education in all regions of Ukraine.

The Diia.Osvita project faces a number of challenges, including ensuring accessibility for all citizens, the digital and educational gap, and limited technical infrastructure in certain regions. Key objectives include motivating users to learn, attracting qualified teachers, updating content in line with current technological trends, funding and supporting the development of the platform. The need for practical tasks, especially for technical and medical specialties, is particularly important. Cybersecurity and personal data protection issues require additional attention.

The Diia.Osvita Project, in general, plays a pivotal role in the development of digital education in Ukraine and preparing the population for the requirements of the modern digital economy. Overcoming mentined challenges will contribute to the effective integration of Diia.Osvita into the digital education system of Ukraine.

Digitalization of HealthCare

The Electronic Healthcare System (eHealth) is designed to automate the billing of medical services and manage medical information in electronic form. Its primary function is to unify, consolidate and protect all medical information and data throughout the country.

According to Article 3 of the Law of Ukraine “Fundamentals of the Legislation of Ukraine on Health Care” an Electronic Healthcare System is defined as an information and communication system that automates accounting of medical services and management of healthcare information, including medical information. The system enables the creation, posting, publishing, and exchange of information, data, and documents in electronic form. It includes a central database and electronic medical information systems, between which the automatic exchange of information, data and documents through API is ensured.

The Electronic Healthcare System (**eHealth**) consists of two components:

- The Central Database (CDB), which is owned by the state, contains software modules and registries for managing, storing and exchanging health information. The CDB enables the exchange of information and documents between the registries in the CDB and other health registries, state electronic information resources of other authorities, and electronic medical information systems.
- Electronic medical information systems, a term that encompasses a variety of private software products. These products automate the work of business entities in the healthcare sector, creation, viewing, and exchange of information in electronic form.

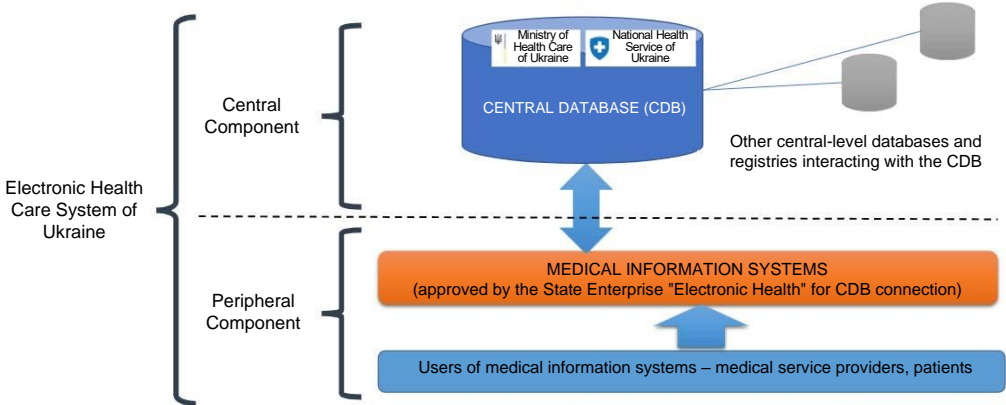


Fig. 6. Architecture of the Electronic Health Care System

Thus, the eHealth architecture is a two-component system consisting of a central state database and electronic health information systems. The state establishes standards and ensures security, while business provides services to users.

One of the medical information systems within eHealth is Helsi. It facilitates the implementation of the Medical Guarantee Program and provides patients with the ability to make appointments, view medical data and receive electronic prescriptions. Helsi is used by patients to make appointments, view medical data and other services, as well as by doctors and medical institutions to automate workflows. Helsi interacts with a central eHealth database to exchange information and ensure a seamless healthcare experience.

Consequently, eHealth emerges as the primary tool of implementing a new approach to healthcare financing and ensures the exchange of medical information among the various registries and healthcare facilities. Helsi operates as an integral component of eHealth, providing interaction between healthcare facilities and CDB for the provision of healthcare services and management of medical information.

The Ministry of Digital Transformation of Ukraine and the Ministry of Health of Ukraine within the EGAP Program implemented by the Eastern Europe Foundation with the support of the Swiss Government have implemented an electronic system of rating distribution to internships based on the Diia.Engine platform. The system automatically calculates the rating of medical graduates based on academic performance for all years of study, Objective Structured Clinical Examination (OSCE), and KROK medical exams (KROK-1 / KROK B, KROK-2). It offers available internship places throughout the country, provides a choice and automatically generates electronic documents for internships. The system is integrated with the vacancy portal of medical institutions.

Mokhova I., Tokarenko V (2020) considered experience in the use of electronic services in healthcare of EU countries. It was discovered that EU's electronic services are being consolidated into a single web portal that will provide a wide range of e-services throughout the EU. They have identified the main obstacles to the development of electronic trust services in the healthcare sector healthcare: privacy and security, lack of integration, information exchange, introduction of standards, increase in capacity, support for new analytical methods.

Romanenko (2025) analyzed the benefits and challenges of eHealth implementation and suggested ways to overcome the threats. E-health optimizes administrative processes in medical institutions, automates document flow, improves resource management and the quality of medical services, and ensures continuity of patient care. The use of electronic health records and artificial intelligence facilitates better diagnosis, while telemedicine expands access to medical services, especially in remote regions. The automation of financial processes contributes to the efficient allocation of budget funds.

Despite the significant benefits, eHealth adoption comes with a number of challenges, including the high financial cost of software implementation, the need to train staff, upgrade infrastructure, and ensure cybersecurity and data protection. Healthcare organizations are becoming targets for cyberattacks, which requires compliance with international standards such as GDPR. Low digital literacy among staff makes adaptation difficult, requiring additional training and technical support.

The possible solutions to address the aforementioned threats are 2FA

authentication, biometric technologies, cryptography for protection data in transit (SSL/TLS) and at rest (AES, RSA), (IDS/IPS), next-generation firewalls (NGFW), role-based access control (RBAC), incident response plans, anomaly detection technologies such as SIEM (security information and event management), etc.

Interactive Science Museums.

An example of the integration of education, science and modern digital technologies is the opening of Interactive Science Museums (ISM). A comparative study of the historical development and activities of modern ISM, highlighting their main features and characteristics is carried out by Slipukhin I.A. et al (Slipukhin I.A., Savchenko Ya.V., Karamanov O.V., 2023).

In September 2020 the first state “Science Museum” of Junior Academy of Sciences of Ukraine was founded in Kyiv.

The Museum of Science (<https://sciencemuseum.com.ua/>) is the first public interactive museum in Ukraine, offering visitors the opportunity to engage with exhibits through tactile exploration, solve puzzles, and participate in scientific experiments. The interactive space presents the most important scientific achievements of humankind, their laws and interactions in a comprehensible and accessible manner.



Fig. 7. Exhibits in the first state “Science Museum” of Junior Academy of Sciences of Ukraine

Source: <https://sciencemuseum.com.ua/>

The project was implemented with the support of the Ministry of Education and the Junior Academy of Sciences of Ukraine. The museum’s collection includes exhibits from the United States, Canada, the United Kingdom, Sweden, and Poland, thanks to the cooperation of the Junior Academy of Sciences of Ukraine with the International Association of Science and Technology Centers.

In December of 2023 an Interactive Science Museum at National University “Yuri Kondratyuk Poltava Polytechnic” (<https://nupp.edu.ua/page/muzey-nauki.html>) was opened. This museum serves as an interactive space, offering a comprehensive presentation of scientific discoveries made by humankind, inventions of Poltava Polytechnic scientists, and the evolution of scientific progress. The museum’s approach is characterized by its accessibility and engaging nature, aiming to provide a captivating and informative experience for visitors.



Fig. 8. Exhibits in Interactive Science Museum at National University “Yuri Kondratyuk Poltava Polytechnic”

Source: <https://nupp.edu.ua/page/muzey-nauki.html>

The project was implemented in cooperation with the National Center “Junior Academy of Sciences”, the first state “Science Museum” of the National Academy of Sciences of Ukraine, the municipal institution of the Poltava Regional Council “Junior Academy of Sciences” and the Startup School of Poltava Polytechnic. The objective of foundation of the Science Museum of Poltava Polytechnic University was to popularize high-tech professions and specialties, to promote advanced study of mathematics, physics, chemistry, biology, and related fields. The activity of the museum contributes to the popularization of science among the youth of Poltava region.

The interactive Science Museum has become the most visited scientific and educational space in the city. Since its opening, the Museum of Science has been visited by more than two thousand schoolchildren and city residents.

Digital Accessibility (Barrier-Free Access)

Digital Accessibility is the concept of equal access to digital technologies, services and information for all individuals, irrespective of their physical ability, age, digital literacy or social status.



Fig. 9. Key Aspects of Digital Accessibility

In Ukraine, digital and information accessibility are two of the six areas of the National Strategy for Creating a Barrier-Free Space in Ukraine by 2030.

Therefore, the issue of digital accessibility as part of the overall strategy for creating a barrier-free space is regulated by the following legislative acts:

1. Decree of the President of Ukraine “On ensuring the creation of a barrier-free space in Ukraine”.
2. UN Convention on the Rights of Persons with Disabilities.
3. National strategy for barrier-free environment in Ukraine until 2030.
4. Resolution of the Cabinet of Ministers of Ukraine No. 757 “Some Issues of Accessibility of Information and Communication Systems and Documents in Electronic Form”.

International Directives include EU Directive 2016/2102 on the accessibility of websites and mobile applications of public authorities, EU Directive 2019/882 on accessibility requirements for products and services (“European Accessibility Act”), Web Content Accessibility Guidelines etc.

The United Nations Development Program in Ukraine in collaboration with the Ministry of Digital Transformation of Ukraine implemented a project “Digital, Inclusive, Accessible: Supporting the Digitalization of Public Services in Ukraine. The project received funding from Sweden and support from the Government of Japan.

Popov D. (2023) presented the findings of a study on the Digital Accessibility legislation of the European Union and several European countries, including Denmark, Germany, France, Sweden, and the United Kingdom. The study was conducted within the framework of the project “Digital, Inclusive, Accessible: Supporting the Digitalization of Public Services in Ukraine”. The report analyzes key EU directives, as well as legislative acts of selected countries, related to web accessibility of products and services, equality of rights, opportunities, participation and citizenship of people with disabilities, and protection of their rights. Consequently, the report provides recommendations for the implementation of specific European practices within Ukrainian legislation, with the objective of ensuring digital accessibility in Ukraine.

Table 5. Key legislative acts of EU countries

Country	Legislative act
Denmark	Web Accessibility Act, implementing EU Directive 2016/2102. Accessibility Requirements of Products and Services, implementing European accessibility act (EAA)
Germany	Act on Equal Opportunities for Persons with Disabilities (BGG) The Barrier-Free Information Technology Ordinance (BITV) The German Accessibility Improvement Act (BFSG) Ordinance on the Accessibility Improvement Act (BFSGV)
France	French Law 2005-102, RGAA and Web Accessibility (Article 47 – Law No. 2005-102 of February 11, 2005 for equal rights and opportunities, participation and citizenship of people with disabilities) as amended by Law No. 2023-171 of March 9, 2023 Order dated 20.09.2019 on the General Regulatory Framework for Improving Accessibility French Labor Code Law No. 2023-171 «Provisions for Adaptation to European Union Law in

	Economic and Financial Matters (Chapter IV: Provisions relating to the accessibility of products and services (Article 16., transposing European Directive no. 2019/882)
Sweden	Act (2018:1937) on accessibility to digital public services, implementing EU Directive 2016/2102 Act (2023:254) on the availability of certain products and services, implementing EU Directive 2019/882
United Kingdom	Equality Act (2010) The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018

Popov D. (2023) also presented a study on use of assistive technologies by individuals with disabilities conducted by the UN Development Program in Ukraine and the National Assembly of People with Disabilities within the framework of the project “Digital, Inclusive, Accessible: Supporting the Digitalization of Public Services in Ukraine”. The report analyzed how people with disabilities, particularly the visually impaired, use assistive technologies, the challenges they face, and unmet needs. A comparative analysis of Ukrainian-language text-to-speech technologies was also conducted.

Survey results showed that only 17% of respondents had access to all necessary technologies. The most critical but unavailable technologies included ATMs with voice output, medical devices with voice support (e.g., thermometers, blood pressure monitors, glucometers), improved Ukrainian speech synthesizers, Braille displays, and paid screen readers. The report also explored the potential of artificial intelligence (AI) in assistive technologies to support individuals with disabilities, such as image recognition, subtitles, and transcription.

Additionally, the study highlighted accessibility issues, particularly the rise of “accessibility overlay” solutions that claim to fix website accessibility using AI. However, the European Disability Forum (EDF) and the International Association of Accessibility Professionals (IAAP) issued a joint statement explaining the limitations of this technology and warned that these overlays do not ensure real accessibility or compliance with European regulations.

Development of electronic communication network

The electronic communications sector is a field of activity related to the provision and reception of electronic communications services, provision of and access to electronic communications networks.

According to the Law of Ukraine "On Electronic Communications," electronic communication is defined as the transmission and/or reception of information, irrespective of its type or form, in the form of electromagnetic signals using technical means of electronic communication. Electronic communications are an integral part of Ukrainian industrial and social infrastructure, the infrastructural basis for digital transformation and development in all sectors of the economy and society.



Fig. 10. Electronic Communications Sector of Ukraine

The infrastructure basis of the electronic communications sector in Ukraine is electronic communications networks, which can be conditionally divided into four main segments (Fig. 11):



Fig. 11. Structure of Ukrainian Electronic Communications

The regulatory framework for electronic communications is outlined in the following documents:

1. The Law of Ukraine “On Electronic Communications”. This law was adopted in December 2020 and came into force on January 1, 2022. It defines the terminology used in the field of electronic communications. It introduces the principle of minimum necessary and predictable regulation of the industry, as well as the notification principle of registration of business entities in the field of electronic communications.

2. The Law of Ukraine “On the National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum and the Provision of Postal Services”. This law defines the legal status of the National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum and the Provision of Postal Services (NCCIR), which is a state regulatory body in the field of telecommunications, informatization, use of radio frequency resources and postal services.

NCCIR is responsible for the regulating activities in the field of electronic communications and ensuring the fulfillment of tasks established by national legislation and international legal obligations.

In order to implement these legislative acts, “Strategy for the Development of the Electronic Communications Sector of Ukraine” has been developed. The Strategy is aimed at promoting efficient investment and innovation in infrastructure and technology to ensure uninterrupted communications for all service users. It provides for the development of high-speed networks and the improvement of service quality. The Strategy is also aligned with the National Strategy for Creating a Barrier-Free Space in Ukraine by 2030.

The Strategy notes the necessity to implement EU regulations in the field of electronic communications into the national legal system in accordance with the Association Agreement with the EU, including synchronization with the European Green Deal. According to the Ministry of Digital Transformation, the integration and use of EU digital market tools will allow to obtain from 2.4 to 3.4 billion dollars in goods and up to half a billion dollars in services.

Challenges of innovative digital tools

The use of innovative digital tools is associated with various problems and challenges. The following potential risk groups include technological, lack of legal regulation, privacy and data protection, market, etc.

Table 6. Challenges of innovative digital tools

Challenge type	Description	Example	Mitigation measures
Technological	Technical errors Cyberattacks, that can lead to the loss or theft of data, as a result, the trust of users.	Cyberattack on the state registries in December 2024 Cyberattack on the Ukrainian railway registries in March 2025 Incident with The DAO project	Implementation IDS/IPS, NGFW, RBAC. Creation of cyberattack response teams, automated incident response system. Using of anomaly detection technologies such as SIEM Audits of system
Lack of legal regulation	Basis on insufficiently regulated technologies and market models, which creates risks for investors and facilitates financial manipulation Impact of legislative changes, that can change market	Uncertain legal status of smart contracts Prohibition of Russian software Regulatory pressure on TikTok in US and Europe	Legislative measures in accordance with the identified threats Study and adaptation of international experience Harmonization with EU and NATO standards

	conditions or prohibit certain products	(2023-2024)	
Confidentiality and data protection	Problems with confidentiality and protection of personal data	Problems with Clearview AI Data leak in Yahoo 2014 Data leak in CAM4 2020	Creation of a comprehensive information security system Conducting of systematic, cybersecurity and information security, cyber hygiene trainings Regular audits of system Strengthen cybersecurity protocols through blockchain, encryption, and zero-trust architectures Draft Law on Amendments to Certain Laws of Ukraine on Information Protection and Cyber Defense of State Information Resources and Critical Information Infrastructure (Reg. No. 11290). Law of Ukraine “On the Protection of Information in Information and Communication Systems”
Market challenges	Significant impact on success of innovative tools of market conditions and trends Absence of a sufficient historical data for new tools as basis for analysis and detection of unusual activity that could be a sign of crime or attack	Disruptions in the online banking of SVB and other banks due to massive withdrawal requests during the banking crisis (Silicon Valley Bank, 2023)	Adaptive AI-driven risk models that continuously analyze new trends and detect anomalies. Real-time monitoring to adjust risk parameters based on market fluctuations. Using of historical proxies and synthetic data to compensate for the lack of long-term records

Conclusions. The digitalization public authorities and public sector in Ukraine contributes to the modernization of public administration and the improvement of public service delivery. It ensures transparency and accountability of government agencies, simplifies administrative procedures, optimizes costs, and reduces corruption risks. Due to digital technologies, public services are becoming more accessible, especially to remote regions, and the interaction between the state, business, and citizens is significantly improving.

Development and implementation of user-friendly online platforms, such as Diia portal and app, are among the key success factors digitalization of Ukraine. An important role is played by the constant expansion of the available electronic services list, which

allows citizens and businesses to interact more effectively with the state. A high level of public engagement in digital interaction also contributes to the successful development of e-governance. Despite the difficulties of martial law, Ukrainian digital infrastructure demonstrates resilience, ensuring the continuity of public services.

However, digital transformation is accompanied by a number of challenges, including cybersecurity, lack of digital literacy, legal restrictions, and significant financial costs for infrastructure upgrades. It is important to guarantee protection of personal data, adapt legislation to modern digital realities, and bridge the digital divide among the population.

Further development requires the introduction of innovative technologies, enhanced interagency integration, and improved government regulation.

References:

- UN E-Government Knowledgebase. URL: <https://surl.li/bjfojg>
- Trembita.gov.ua – звіт за 1-й квартал 2023 року. URL: <https://surl.li/zrsriz>
- Національний реєстр електронних інформаційних ресурсів. URL: <https://se.diia.gov.ua/nreir>
- Попович М.В. (2024). Особливості ведення єдиного реєстру досудових розслідувань (ЄРДР) та інформаційно-телекомунікаційної системи на етапі досудового слідства // Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. Випуск 85: частина 4, 2024. С. 393-398. DOI: <https://doi.org/10.24144/2307-3322.2024.85.4.58>
- Національне бюро відновило роботу системи електронного кримінального провадження eCase MS. URL: <https://surl.li/tgacbw>
- EUACI. Проведення обстеження щодо впровадження електронної системи управління кримінальними справами eCase. URL: <https://surl.li/jvoadg>
- Барич-Тіновська Л., Дурман О. (2022). Сучасні цифрові інструменти підвищення прозорості та ефективності використання публічних коштів // Таврійський науковий вісник. Серія: Публічне управління та адміністрування. № 3, 2022. С. 14-22. 10.32851/tnv-pub.2022.3.2. DOI: <https://doi.org/10.32851/tnv-pub.2022.3.2>
- Криниця С. (2024). Digitalization Strategies of the Public Financial Management System in Ukraine: Analysis and Perspectives // Acta Academiae Beregsasiensis. Economics. Pp. 307-321. DOI: 10.58423/2786-6742/2024-6-307-321.
- Стратегія здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року. Розпорядження Кабінету Міністрів України від 17 листопада 2021 року № 1467-р. URL: <https://zakon.rada.gov.ua/laws/show/1467-2021-%D1%80#Text>
- Стратегія реформування системи управління державними фінансами на 2022-2025 роки. Розпорядження Кабінету Міністрів України від 29 грудня 2021 року № 1805-р. URL: <https://zakon.rada.gov.ua/laws/show/1805-2021-%D1%80>
- Krynysia S. (2024). Digital dividends of the digitization of public finance management system // Причорноморські економічні студії. Випуск 88, 2024. С. 51-58. DOI: <https://doi.org/10.32782/bses.88-8>
- Farooq Kh., Solowiej B. J. Artificial Intelligence in the Public Sector: Maximizing Opportunities, Managing Risks : World Bank Group. URL: <https://surl.li/jnhnul>
- Organisation for Economic Co-operation and Development (2024) Using Artificial Intelligence in Public Financial Management 46th Annual Meeting of the Committee of Senior Budget Officials. URL: <https://surli.cc/mgpajg>
- Collosa A. Use of Big Data in Tax Administrations. CIAT – Inter-American Center of Tax Administration. 2021. URL: <https://surl.li/cixppc>
- Krynysia S. Leveraging big data technologies for enhanced public participation in public financial management // Фінансово-кредитна діяльність: проблеми теорії і практики. Том 3. № 56, (2024). Pp. 186-203. DOI: <https://doi.org/10.55643/fcартп.3.56.2024.4402>
- Станкевич А.В. Смарт-договори як вид електронних договорів, їх особливості та проблематика при

- електронному обігу об'єктів цивільного права // Науковий вісник Ужгородського Національного Університету. Серія Право. Випуск 87. Ч. 1, 2025. С. 288 – 292. DOI: <https://doi.org/10.24144/2307-3322.2025.87.1.42>
- Ranked: The Top 25 Countries with the Most Data Centers. URL: <https://surl.li/yonsca>
- Boost Portal. URL: <http://boost.worldbank.org/boost-initiative>
- Basiuk O. P. (2022). Digital technologies in optimization of the budget process: best international experience and conclusions for Ukraine. Pressing Problems of Public Administration, 1(60), 116–131. DOI: <https://doi.org/10.26565/1684-8489-2022-1-08>
- Kondrat O. (2024) Innovative financial tools in the enterprise development system. Ukrainian Journal of Applied Economics and Technology. 2024. Volume 9. № 1, pp. 339 – 344. DOI: <https://doi.org/10.36887/2415-8453-2024-1-57>
- Сергієнко О.А., Самусь П.О. (2023) Аналіз поточного стану правового регулювання цифрових смарт-контрактів в Україні та в світі // Usage of blockchain technologies in energetics – 2023 : coll. of materials of the scientific and practical conf. – К.: ПІМЕ ім. Г. Є. Пухова НАН України, 2023. – С. 58-60. URL: <https://surl.li/qjgglg>
- Некіт К. (2021) Переваги та недоліки смарт-контрактів як підстав виникнення права власності // ВІСНИК НТУУ «КПІ». Політологія. Соціологія. Право. Випуск 3 (47), 2020. С. 101-105. DOI: [https://doi.org/10.20535/2308-5053.2020.3\(47\).229494](https://doi.org/10.20535/2308-5053.2020.3(47).229494)
- Іванов А.М., Шмига В.О. (2022). Смарт-контракти у договірних відносинах: реалії та перспективи використання // Юридичний науковий електронний журнал. № 4, 2022. С. 150–152. DOI: <https://doi.org/10.32782/2524-0374/2022-4/32>
- Кривенко Ю.В. (2023). Щодо поняття та ознак смарт-контракту // Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція. № 64, 2023. С. 80-83. DOI: <https://doi.org/10.32841/2307-1745.2023.64.16>
- Чекіна В.Д., Князев С.І. (2019) Аналіз впливу big data and analytics на реальний і державний сектори економіки та проблеми їх оцінювання за допомогою статистичних методів // Економіка промисловості. № 1 (85), 2019. С. 51–64. DOI: doi.org/10.15407/econindustry2019.01.051
- Вакшинська Н.Ю., Шандрівська О.Є. Специфіка розвитку ринку big data для потреб відновлення економіки України в поствоєнний період // Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку № 2 (9), 2023. С. 244-256. DOI: <https://doi.org/10.23939/smeu2023.02.244>
- Державні реєстри України зазнали масштабної кібератаки: скільки триватиме відновлення. URL: <https://surl.li/mndmfv>
- Iran, Russia and North Korea changed cyber attack tactics in the last year, says Microsoft. URL: <https://surl.li/iewodr>
- Грицяк Н.В., Твердохліб О.С. (2020). Практичні аспекти застосування технологій аналізу даних великих масивів (Big Data) в публічному управлінні // Ефективність державного управління. Випуск 3 (64). Ч. 1, 2020. С. 121–135. DOI: <https://doi.org/10.33990/2070-4011.64.2020.217610>
- Blinova H. Legal principles of using electronic information resources in the concept of the digital state // Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування. № 2, 2021. С. 53-60. DOI: <https://doi.org/10.54929/pmtl-issue2-2021-10>
- Програма великої трансформації: «Освіта 4.0: український світанок». URL: <https://surl.li/dttnoo>
- Бохоцько Є.О., Шелевер О.В., Дерека К.О. (2023). Digital Transformation of Education 4.0: Teaching and Learning in the Age of Digital Technologies // Інноваційна педагогіка. Випуск 60, 2023. С. 219-222. DOI: <https://doi.org/10.32782/2663-6085/2023/60.45>
- Малицька І.Д. Розвиток цифрової грамотності вчителів під час воєнного стану (підтримка ЮНЕСКО) // Звітна наукова конференція Інституту цифровізації освіти НАПН України «Цифрова трансформація освіти України в умовах воєнного стану»: зб. матеріалів. ЩО НАПН України, 2023. С. 36-39. URL: <https://lib.iitta.gov.ua/id/eprint/735167/1/Malitska%20ID.pdf>
- Малихін О., Арістова Н., Ліпчевська І. Цифровізація профільної середньої освіти як інструмент мінімізації навчальних втрат учнів в умовах воєнного стану // Український педагогічний журнал. № 4, 2024. С. 57-64. DOI: 10.32405/2411-1317-2024-4-57-64

- Mokliak V., Bondarenko T. (2023) «Diia. Education» platform as an example of gadgetalization in Ukraine // Scientific Papers of Berdiansk State Pedagogical University. Series: Pedagogical Sciences. Vol. 2. 2023. Pp. 79-87. DOI: 10.31494/2412-9208-2023-1-2-79-87
- Стратегія розвитку сфери електронних комунікацій України на період до 2030 року. URL: <https://thedigital.gov.ua/storage/uploads/filesСтратегія:15:05.pdf>
- Мінцифра та МОЗ запустили електронну систему рейтингового розподілу в інтернатуру. URL: <https://surl.li/ysjobe>
- Mokhova I., Tokarenko V. (2020). European experience in the use of electronic services in healthcare // Law and Public Administration. № 2, 2020. Pp. 188-195. DOI: <https://doi.org/10.32840/pdu.2020.2.29>
- Романенко С. (2025). Впровадження електронної медицини в управлінні медичними закладами: переваги та виклики // Інвестиції: практика та досвід. № 4, 2025. С. 256-264. DOI: 10.32702/2306-6814.2025.4.256.
- Сліпучіна І. А., Савченко Я. В., Караманов О. В. (2023) Інтерактивні музеї науки як освітні середовища // Освіта та розвиток обдарованої особистості. № 1 (88), 2023. С. 28-37. DOI: [https://doi.org/10.32405/2309-3935-2023-1\(88\)-28-37](https://doi.org/10.32405/2309-3935-2023-1(88)-28-37)
- Перший державний “Музей науки” Малої академії наук України. URL: <https://sciencemuseum.com.ua/>
- Національний університет «Полтавська політехніка імені Юрія Кондратюка». Музей науки. URL: <https://nupp.edu.ua/page/muzei-nauki.html>
- Розпорядження Кабінету Міністрів України від 14 квітня 2021 р. № 366-р. Про схвалення Національної стратегії із створення безбар’єрного простору в Україні на період до 2030 року. URL: <https://surl.li/bmhdxc>
- Попов Д. Законодавче регулювання цифрової безбар’єрності: найкращі європейські практики. Звіт за результатами дослідження. URL: <https://surl.li/rkxoyr>
- Попов Д. Використання допоміжних технологій людьми з інвалідністю. Звіт за результатами дослідження. URL: <https://surl.li/xphxwv>
- Accessibility overlays don’t guarantee compliance with European legislation. URL: <https://surl.li/ecgcuh>
- Закон України «Про захист інформації в інформаційно-комунікаційних системах». URL: <https://surl.li/ocggkm>

CHAPTER 12. INFORMATION SECURITY IN THE GLOBAL CONTEXT: LINGUISTIC PERSPECTIVES AND THE ROLE OF ENGLISH

Liudmyla IBRAHIMOVA

senior English language lecturer

Vinnitsia National Technical University, Department of Foreign Languages,
(95, Khmelnytske shose, Vinnitsia, 21021, Ukraine)

milatulchak@gmail.com

<https://orcid.org/0000-0002-9265-2449>

Svitlana NYKYPORETS

senior English language lecturer

Vinnitsia National Technical University, Department of Foreign Languages,
(95, Khmelnytske shose, Vinnitsia, 21021, Ukraine)

fotinia606@gmail.com

<https://orcid.org/0000-0002-3546-1734>

Abstract. This article addresses the multifaceted relationship between information security, the English language, and the educational sphere in modern Ukraine. The ongoing Russian war of aggression has significantly heightened the destructive impact of disinformation targeting both global and domestic audiences. The primary research problem centres on the growing vulnerability of citizens – especially language learners – to manipulative narratives and misinformation campaigns disseminated in English. Our study investigates the pedagogical methods that integrate critical thinking and authentic English-language materials to shield learners from such threats. The theoretical framework draws on sociolinguistics, discourse analysis, and best practices in foreign language teaching, reflecting the urgency of media literacy in conflict settings. Crucially, we highlight the pivotal role English teachers play in equipping students with evaluative and analytical tools for detecting bias and inaccuracies in real-world content. Concrete effectiveness of these methods is illustrated through case studies involving mainstream news outlets, social media feeds, and targeted fact-checking exercises. Results indicate a marked improvement in students' language proficiency, critical awareness, and capacity to critically assess narratives related to the Russian-Ukrainian conflict. By cultivating both advanced linguistic competence and informed digital literacy, this educational process empowers learners to become active participants in Ukraine's global discourse. Overall, the findings underscore the need for continued research and curricular innovation, asserting that robust information security education significantly enhances Ukraine's resilience on the world stage.

Key words: intercultural communication, disinformation, English language curricula, cultural awareness, resilience.

Information security, in its broadest sense, transcends the mere deployment of firewalls, encryption algorithms, and cybersecurity protocols. It is an intricate tapestry woven from a confluence of technical expertise, policy considerations, sociocultural norms, and, crucially, linguistic variables. While technology often finds itself at the forefront of

discussions about preventing data breaches and safeguarding intellectual property, it is language – how it is used, understood, and translated – that underpins the success or failure of communication in global information security networks. In a world that is increasingly interconnected through digital platforms, the capacity to facilitate clear, nuanced, and context-appropriate exchanges is central to securing data. Indeed, complexities in linguistic usage can undermine otherwise robust security frameworks, as errors or ambiguities in translation can open the door to misinterpretations, vulnerabilities, and even deliberate manipulations. Understanding how languages function within various cultures and how English, as a global lingua franca, shapes professional and casual communication, is thus essential for crafting effective information security strategies.

The linguistic dimension of information security becomes abundantly evident when examining how cybersecurity policies are drafted and shared (*Baltuttis et al., 2024*) across diverse linguistic communities. Although English is predominantly the de facto language in many international technology and security collaborations, the localized interpretations and implementations of such policies are no less crucial than the original directives. Every language possesses its own unique linguistic structures – syntax, semantics, pragmatics, sociolinguistic norms – that colour how individuals understand and respond to information security measures. Consequently, when developers, network administrators, and policymakers communicate in English, but come from distinct cultural-linguistic backgrounds, certain concepts may be conveyed inaccurately, or security protocols may not be consistently enforced. This phenomenon can arise not only from translation difficulties, but also from deeper cultural assumptions embedded in language that produce divergences in risk perceptions and trust boundaries.

These divergent perceptions have material consequences. Consider the ways in which terms such as “privacy,” “data protection,” and “authorized access” may carry subtly different connotations and historical contexts from one language community to another. While English often serves as a neutral or universal vehicle in global business and diplomacy, not every stakeholder possesses equal fluency in it, nor do they approach security discourse in the same manner. Mismatched expectations, arising from limited linguistic proficiency or from culturally rooted styles of communication, can hinder the timely and precise execution of security protocols. Moreover, technical jargon itself – concepts like “encryption key management,” “multifactor authentication,” or “zero-day vulnerabilities” – is often anchored in English. Where direct translations do exist, they sometimes lack the precise nuance that the English term carries, or they rely on borrowed English words that non-native speakers may not fully grasp.

From a policy standpoint, this raises an intriguing set of questions: How should guidelines for secure data handling be adapted to multiple languages without sacrificing clarity? What is the responsibility of global organizations, such as multinational corporations or intergovernmental agencies, to ensure the accuracy of translations and the cultural appropriateness of security instructions? How do local norms and linguistic practices shape employees’ willingness to report potential threats, abide by strict password regulations, or adhere to guidelines for remote work security? These are not purely linguistic or sociocultural curiosities; they lie at the heart of the effective or ineffective functioning of worldwide information security systems.

At the same time, the ascendancy of English as a global lingua franca in technology and cybersecurity is not merely incidental. A major driver behind this dominance is the historical development of internet-based communication, initially pioneered by English-speaking institutions and companies in North America and Western Europe. Over time, English solidified its status as the language of programming, tech entrepreneurship, and international research collaboration. Yet, this centrality of English also codifies power relationships. It can inadvertently marginalize non-English-speaking communities, limiting their direct involvement in vital decision-making processes and in real-time threat sharing. Overcoming or mitigating these disparities requires a more nuanced approach – one that acknowledges the role of English while simultaneously respecting and incorporating the linguistic diversity of the international security landscape.

In the broader global context, cyber-threat actors do not restrict themselves to an Anglophone universe. Malicious entities frequently exploit linguistic gaps and variations in phishing emails, social engineering attacks, or well-targeted phone scams. Furthermore, international cybercriminals may take advantage of the fragmented nature of security communication. If official advisories are issued solely in English, certain populations are left relatively uninformed and thus more vulnerable. Indeed, entire networks, industries, or countries might become “soft targets” if security protocols are misunderstood or incorrectly translated. This phenomenon underscores the practical and urgent imperative to address language as a significant factor in global information security.

Equally critical is the recognition that linguistics is more than just translation. We are dealing with pragmatics, which concerns how language is used in context. For example, the norms of politeness and directness in certain cultures can lead individuals to hesitate before flagging suspicious online behaviour if they fear it might cause interpersonal conflict. Similarly, some cultures may value hierarchical communication patterns, where subordinates do not question superiors, even if they notice a potential security weakness. Such sociolinguistic patterns can create blind spots or communication bottlenecks in an organization’s security apparatus. Even the creation of user interfaces for security systems involves carefully chosen wording to ensure that instructions are correctly understood and that the user’s cultural-linguistic expectations are met. Ignoring these intricacies can compromise the universal adoption of best practices in information security. Consequently, ensuring multilingual accessibility in cybersecurity advisories and training materials is crucial for comprehensive global protection. Such vulnerabilities highlight the necessity for cross-cultural collaboration and specialized translation expertise in every stage of cybersecurity planning.

1. Specificity of information threats in international communication in the world

This article’s purpose is to explore these multifaceted issues by examining both the linguistic and cultural dimensions of information security, while simultaneously highlighting the central, and sometimes problematic, role of English. In doing so, our goal is to advance the conversation beyond purely technological or purely policy-oriented frameworks. While hardware and software solutions are, of course, indispensable to modern cybersecurity, they operate within a matrix of human interactions that are continuously shaped by language. A policy drafted in English but improperly localized could hinder, rather than help, an organization’s security posture. By the same token, a well-translated but

culturally misaligned guideline could still fail to elicit the intended behavioural response, thereby leaving vulnerabilities in place.

In the pages that follow, we will explore how linguistic research methods, including discourse analysis and pragmatics, can help uncover hidden assumptions in cybersecurity literature and policy documents. We will likewise investigate how cultural-linguistic norms in different societies impact the efficacy of security awareness training. Special attention will be given to real-world case studies that illustrate the direct effects of linguistic misunderstanding on organizational vulnerabilities. These may include instances of phishing emails exploiting certain culturally specific tropes or formal registers, as well as cases where a lack of clear linguistic guidance has led to catastrophic lapses in data protection. We will then turn our attention to the future, offering recommendations that draw on linguistic scholarship to propose more robust and culturally sensitive approaches to information security.

In highlighting the critical role of English, we do not seek to diminish its undeniable utility as a global medium. Rather, we aim to shed light on the ways in which its global dominance can be both an asset and a constraint. English connects multinational teams, but it may also inadvertently exclude or misinform those who have varying levels of English proficiency. We therefore assert that addressing global information security necessitates the integration of linguistic expertise at all levels: from the drafting of security protocols to the training of users in culturally diverse workplaces. Effective cybersecurity strategies depend not only on the adoption of cutting-edge encryption standards or the most advanced intrusion detection systems, but also on accurate, context-sensitive communication that resonates with diverse linguistic audiences around the world.

Recent scholarly discourse underscores the urgent need to equip language learners with critical thinking skills and robust information literacy, particularly in contexts of conflict and heightened propaganda. An influential milestone in understanding the structural features of disinformation is Wardle and Derakhshan's seminal report, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking* (Council of Europe, 2017), which details the typologies of misinformation, disinformation, and malinformation. Their taxonomy forms the basis for numerous subsequent studies, including Hobbs's (Hobbs, 2023) exploration in her book of "*Media Literacy and Media Education Research Methods*", which focuses on language-based strategies to identify and mitigate deception within online discourse communities. Li (Li, 2016), writing in *Contemporary Educational Psychology*, provides empirical data on how classroom interventions can bolster critical reading among learners grappling with multilingual media environments – a point of particular relevance to Ukraine, where both local-language and foreign-language propaganda intersect. Meanwhile, Cristiano et.al. (Cristiano et. al., 2023), in *Journal of Cyber Policy*, foregrounds how digital literacy initiatives can help reduce vulnerability to manipulative narratives in conflict zones.

Although these works illuminate critical areas – such as building resilience against disinformation and fostering higher-order thinking in foreign language classes – they often do not address in enough depth the unique sociolinguistic realities confronted by teachers and students in active conflict regions. This is particularly true for Ukraine, where learners regularly engage with English-language media both for academic and practical survival-oriented purposes. Existing analyses have identified the pedagogical potential of authentic

materials (*Chinn, 2020*) and the importance of fact-checking tools (*UNESCO, 2022*) Global Media and Information Literacy framework. However, few empirical studies detail how these recommendations are implemented amid wartime upheavals, infrastructural disruptions, and continuous psychological stressors.

To bridge these gaps, the present study leverages both the foundational theoretical insights from Wardle and Derakhshan and Hobbs and the applied frameworks proposed by Cristiano. Specifically, it expands on how Ukrainian educators – operating in an environment saturated with Russian propaganda – can contextualize critical language instruction to facilitate effective detection of manipulative messages. By integrating micro-level classroom strategies (debates, case studies, and targeted source analysis) with macro-level considerations (institutional support, access to reliable digital resources), the article examines the feasibility and efficacy of existing methods. Thus, while prior scholarship lays the groundwork for teaching critical thinking alongside language skills, this study addresses previously unsolved parts of the general problem: the design, implementation, and systematic evaluation of structured classroom interventions in a high-stakes conflict environment. The goal is to offer evidence-based practices that are both culturally sensitive and adaptable, contributing to the broader conversation on how foreign language pedagogy can serve as a frontline defence against pervasive disinformation.

In essence, information security cannot be divorced (*Brown, 2022*) from language. Every alert, every security policy update, every incident report, and every piece of user education must be conveyed in a language and style that is comprehensible, relevant, and actionable. Otherwise, the best technological safeguards can be unwittingly compromised by human error, cultural misunderstandings, or linguistic oversights. By integrating linguistics into our approach to cybersecurity, we can construct a more inclusive, secure, and resilient global digital environment, better equipped to handle the sophisticated and evolving threats of the modern era. Our mission, therefore, is to reveal how a deeper engagement with linguistic perspectives – including a critical view of English's centrality – can strengthen the international community's collective capacity for information security.

In the contemporary digital era, the concept of 'information threat' has emerged as a critical focal point for researchers, policymakers, and the general public. While technological progress has afforded unprecedented opportunities for global outreach and knowledge exchange, it has also birthed sophisticated methods of manipulating and distorting information. Information threats, at their core, involve the deliberate dissemination of misleading or harmful data – ranging from orchestrated disinformation campaigns to well-planned cyberattacks aimed at stealing sensitive material or shaping public perception. These threats operate across borders, languages, and sociocultural contexts, highlighting the urgent need for a multidimensional approach that addresses not only technical vulnerabilities but also linguistic and cultural nuances.

Against this backdrop, English frequently occupies centre stage due to its position as a global lingua franca. Whether it is in the realm of social media, international diplomacy, global commerce, or higher education, English has become the language through which key policies are debated, commercial deals are struck, and public opinions are often moulded. This widespread adoption arises partly from historical factors, notably colonial expansion and the influence of English-speaking nations in technological innovation and media. More recently, the internet's early development in predominantly English-speaking environments

contributed further to the language's proliferation online. Consequently, English is not only a vehicle for exchanging information but also a powerful medium through which nefarious actors can deploy strategic misinformation, launch cyberattacks, and conduct subtle manipulation aimed at reshaping public discourse or sowing social discord.

In essence, understanding information threats in the world demands a grasp of how language functions within those threats. Because English has been woven so tightly into global communication channels, vulnerabilities that arise in English-speaking contexts often reverberate worldwide. Furthermore, knowledge of English is not uniform – even in regions where English is widely understood, varying levels of fluency can open the door to different forms of exploitation. This reality underscores the need for critical language awareness and robust strategies that account for linguistic diversity, as well as for the continuously evolving nature of malicious information tactics.

Disinformation. Definition and difference from propaganda

Disinformation, by its most accepted definition, is false or misleading information that is deliberately created and spread with the intention of causing harm or influencing public opinion. Although sometimes confused with propaganda – a broader term describing information (often biased) used to promote or publicize a particular political cause or viewpoint – disinformation is characterized by its intentional deceit and subversive goals. Propaganda, in contrast, can at times involve selective truth-telling or exaggeration rather than outright fabrication. The key element (*Jowett, 2015*) differentiating disinformation from other forms of communicative persuasion is the deliberate distortion of facts, whether subtle or blatant, to manipulate the perceptions, decisions, or behaviours of a target audience.

Examples of large-scale disinformation campaigns in the world

High-profile instances of disinformation have garnered significant attention and remain a prime concern for governments, non-governmental organizations (NGOs), and citizens alike. In Ukraine and the United States, disinformation campaigns surrounding political elections have illustrated how strategic falsehoods and manipulated narratives can swing public sentiment. Social media platforms, such as *Facebook* and *X(Twitter)*, have been used to distribute misleading stories or sensational claims to both English-speaking domestic audiences and foreign constituencies, exacerbating political polarization and undermining trust in democratic institutions.

In the United Kingdom, the Brexit referendum served as another prominent stage for disinformation. Campaigns on both sides leveraged emotionally charged messages – some verifiably inaccurate – to sway voters uncertain about the economic and social implications of remaining in or leaving the European Union. These examples underscore the potent role that English, used in mainstream media and social platforms, plays in amplifying disinformation across national and international boundaries.

False claims concerning economic benefits and migration policies circulated widely, muddling the facts for many citizens. Social media channels, in particular, became fertile ground for quick, unchecked dissemination of rumours. As a result, the referendum period witnessed heightened polarisation and a surge in anti-expert sentiment. Political figures and campaign strategists harnessed these tactics, capitalising on the emotional resonance of simplistic slogans rather than fostering nuanced debate. In retrospect, the Brexit experience underscores the urgency of developing critical thinking and robust information evaluation

skills among English language users worldwide. Crucially, it also brings into relief the need for heightened oversight and collaboration among digital platforms, governments, and civil society to mitigate the destructive impact of disinformation tactics. Strengthening educational interventions to teach critical evaluation of media content can help guard against similar challenges in other democratic processes worldwide.

Below are three commonly observed manipulation techniques in English-language media and on social media platforms, along with illustrative examples for each. These techniques are by no means exclusive to English-speaking contexts, but given the language’s global reach, they can gain significant traction in shaping public opinion.

Table 1.

Manipulation techniques in media

		Description	How it appears	Example
1.	Bandwagon effect	The bandwagon effect exploits our innate desire to fit in with the majority or be on the “winning side.” Content employing this strategy implies that a particular viewpoint, product, or political stance is universally accepted or overwhelmingly popular.	Headlines or social media posts that claim “ <i>everyone is talking about X</i> ” or “ <i>millions are switching to Y</i> ” can pressure individuals to conform, even when the actual number of people involved is relatively small. By repeatedly insisting that “everyone else” supports a certain viewpoint, the message can nudge fence-sitters into adopting that same stance out of fear of being left out.	A series of social media posts announcing that “ <i>9 out of 10 Americans are outraged by the new policy</i> ” may create the impression of overwhelming consensus. In reality, if the cited statistic is unverified or fabricated, it can still trigger a bandwagon effect, causing readers to assume that a majority shares this sentiment – even when the real figures are unknown or markedly lower.
2.	Appeal to authority	This technique relies on endorsements or citations from high-profile individuals, institutions, or so-called “experts” to legitimize a claim. Rather than focusing on the evidence itself, the audience is encouraged to trust a statement because of who allegedly said it.	By citing “expert opinions,” “top scientists,” or “government insiders,” media outlets or social media personalities can dissuade critical questioning. The mere invocation of authority can quash deeper inquiry, especially when sources are vaguely referenced, unnamed, or only tangentially qualified.	A news segment might declare, “Leading economists warn of impending market collapse,” without specifying which economists, their credentials, or the data supporting their viewpoint. Audiences might accept the statement without further analysis, simply because the term “leading economists” implies a level of authority and expertise.
3.	Sensational or polarizing headlines	Eye-catching headlines that invoke fear, shock, or anger are frequently used to lure readers into clicking on a link or	Phrases like “ <i>You won’t believe what happened next!</i> ” or “ <i>Shocking development reveals massive cover-up!</i> ” are typical of this approach.	An article titled “ <i>Massive scandal rocks parliament-democracy in crisis!</i> ” might turn out to discuss a relatively minor procedural controversy. However, the

		sharing a post. Known as <i>clickbait</i> in online contexts, these headlines often oversimplify complex issues into exaggerated, emotionally charged statements.	While the body of the article might present more nuanced information, the sensationalized title sets a tone that can colour how readers interpret the content.	exaggerated framing fosters outrage or alarm before readers even delve into the details, shaping their subsequent reactions and undermining balanced analysis.
--	--	---	--	--

Source: Created by authors.

Tools and platforms most often used to spread fakes

The digital revolution has democratized information dissemination, making it easier for anyone to publish, share, and circulate content on a global scale. Social networks such as *Twitter*, *Facebook*, *Instagram*, and *TikTok* serve as swift conduits for viral content, including fabricated news stories and manipulated audiovisual material. Moreover, messaging apps like *WhatsApp* and *Telegram* enable disinformation to spread in closed or semi-private circles, which can be particularly difficult for fact-checkers or regulators to monitor. Online forums and video-sharing platforms (e.g., *YouTube*, *Rumble*) also play a role in disseminating conspiratorial content, often in English, as creators aim to reach the largest possible global audience.

Even traditional media outlets can become unwitting participants in the spread of disinformation when they fail to rigorously verify sources or rely on sensational headlines to drive viewer engagement. Consequently, while there has been an upsurge of fact-checking services, the sheer volume of content and the speed at which it circulates can overwhelm efforts to systematically identify and correct falsehoods. In the English-speaking world, where media outlets often command international followings, disinformation can proliferate rapidly and influence audiences far beyond geographic borders.

Cyberattacks. Overview of the main types of cyberattacks

Cyberattacks aim to disrupt, damage, or gain unauthorized access to computer systems, networks, and databases. Several core tactics are particularly prevalent.

Table 2.

Main types of cyberattacks

	Type	Description
1.	Phishing	Attackers pose as trusted entities in emails, text messages, or websites, tricking recipients into revealing sensitive personal or financial information.
2.	Email hacking	Unauthorized access to email accounts allows attackers to steal data, monitor communication, or launch secondary attacks on the user's contacts.
3.	DDoS (distributed denial of service) attacks	Overwhelming a targeted website or network with massive, coordinated traffic spikes, effectively paralyzing its ability to function.
4.	Ransomware	Malicious software that encrypts a victim's data, offering decryption keys only if a ransom is paid.
5.	Malware and spyware	Software designed to infiltrate computer systems, either to disrupt normal operations or covertly gather sensitive information.

Source: Created by authors.

These cyberattacks exploit both technical vulnerabilities (unpatched software, weak passwords) and human vulnerabilities (lack of awareness, poor security habits). As with disinformation, they can be carried out at scale, often transcending national boundaries thanks to the decentralized nature of the internet.

English-speaking countries are frequently prime targets for cyberattacks for several interrelated reasons. Firstly, the global reach and economic influence of markets like the United States and the United Kingdom make them lucrative targets for financially motivated cybercriminals. Secondly, major international companies and technology hubs (e.g., Silicon Valley) are concentrated in English-speaking regions, offering attackers access to valuable intellectual property and significant data repositories. Thirdly, the dominance of English in online communication and business transactions expands the attack surface: malicious actors can execute phishing campaigns, fake websites, and hacking attempts that affect a global user base, regardless of their native language, simply by leveraging English as a universal touchpoint.

Interconnection of cyberattacks and information manipulation

Cyberattacks increasingly dovetail with broader disinformation efforts, producing a multifaceted threat environment. Breached systems can yield sensitive personal or organizational data, which can then be selectively leaked or weaponized in disinformation campaigns. Phishing emails can be tailored to reflect hot-button social or political issues, thus intensifying their persuasive impact. Such synergy between technical breaches and manipulative messaging exemplifies how information threats extend beyond merely stealing data: they can be engineered to reshape public opinion, destabilize markets, or erode trust in institutional frameworks.

Manipulation through information channels

Manipulation within the media space takes on varied forms, each leveraging distinct strategies. While some manipulative tactics rely on emotional triggers, others exploit logical fallacies or psychological pressure. This diversity not only complicates the detection of manipulative messages but also underscores the importance of multi-pronged defence strategies, including critical thinking education and fact-checking tools. Ultimately, a comprehensive approach that addresses emotional, logical, and psychological manipulation is essential for a robust information ecosystem.

Table 3

Forms of media manipulation

	Form	Description	Outcomes
1.	Emotional manipulation	Content crafted to trigger fear, anger, or empathy, prompting impulsive reactions rather than calm deliberation. Headlines that stoke outrage or highlight dramatic personal stories often fall into this category.	1. Impaired reasoning. Strong emotions like anger or fear can lead individuals to make hasty decisions without examining facts in depth. 2. Polarization. People may split into opposing groups, each fuelled by emotional rhetoric that vilifies the “other side,” thereby reducing opportunities for constructive dialogue. 3. Viral spread of content. Emotionally charged posts, headlines, or videos tend to get shared rapidly, amplifying reach and potential misinformation.

2.	Logical (pseudo-logical) manipulation	Presenting incomplete or distorted data in a manner that appears analytical or evidence-based. While the arguments seem logical at a superficial level, deeper scrutiny reveals manipulations of context, correlation-causation fallacies, or cherry-picked statistics.	1. Misled public perceptions. Audiences accept skewed arguments as valid, believing they have engaged with “data-driven” proof. 2. Reinforcement of biases. Faulty logic can confirm pre-existing beliefs, making readers even more resistant to conflicting evidence. 3. Policy or behaviour changes based on false premises. Decisions – whether individual or collective – are made under the illusion of rational support, potentially leading to harmful societal outcomes.
3.	Psychological manipulation	Techniques aimed at exploiting cognitive biases, social identities, or peer pressure. These often draw on authoritative or celebrity endorsements and can influence groupthink dynamics in online communities.	1. Erosion of individual autonomy. People may feel pressured to conform to a group or an authoritative figure, relinquishing personal judgment. 2. Groupthink and echo chambers. Communities can become insular, recycling and strengthening manipulative narratives without outside scrutiny. 3. Manipulated loyalty and identity. By framing issues as central to a person’s sense of belonging, manipulators can secure unwavering loyalty to a cause, reducing the likelihood of questioning or debate.

Source: Created by authors.

Common tactics encountered in English-language news outlets, talk shows, and online platforms include the ‘bandwagon effect’ – implying that a view is ubiquitous so audiences feel compelled to conform – and the ‘appeal to authority,’ where a statement is taken at face value merely because an influential figure or institution endorses it. Moreover, sensational or polarized framing (e.g., “all-or-nothing” narratives) is frequently employed to reduce complex issues into simplistic dichotomies. These methods can be particularly potent in emotionally charged or fast-moving news cycles, where individuals have little time to verify facts or counterarguments.

On social media, memes and short-form videos represent a powerful vector for manipulation. They can distil complicated ideas into digestible visuals, sometimes evoking a sense of humour or shared identity. Because these formats are easy to produce and share, they can quickly gain traction among diverse English-speaking audiences, spreading even further if they tap into existing cultural or political divides.

The influence of language (vocabulary, style) on audience perception and response

Language choice is instrumental in shaping how information is processed. Different vocabulary sets can evoke varied emotional responses, while style (formal vs. informal, academic vs. conversational) can either engender (*Betancourt, 2024*) trust or scepticism. In the English-speaking world, where large populations use English as a second language, connotations of words and idioms may be misconstrued. Malicious entities can exploit these linguistic ambiguities, crafting messages that either appear benign to casual readers or exploit emotional triggers for those deeply embedded in a specific cultural-linguistic context.

For instance, labelling a policy as “revolutionary” might appeal to audiences seeking radical change, while more neutral language like “innovative” might resonate with moderate segments. Similarly, employing inflammatory phrases in headlines can whip up public emotion, driving clicks or shares that boost a piece of content’s reach. In each case, the linguistic register and tone act as catalysts, guiding how audiences interpret and respond to the presented information.

Throughout this exploration of information threats in the English-speaking world, we have seen how disinformation, cyberattacks, and manipulative tactics intersect to create a complex environment that transcends national boundaries. English’s global prominence amplifies these threats by furnishing malicious actors with a linguistically unified platform that can reach vast and diverse audiences. The very qualities that make English essential for international communication and collaboration – ease of transmission, widespread use, and a relatively standardized form – also position it as a potent channel for disinformation and cyber exploitation.

Key to mitigating these hazards is the cultivation of critical thinking skills and heightened language proficiency among users and policymakers. Mastery of English not only facilitates the detection of manipulative linguistic cues but also enables the careful parsing of complex or emotionally charged messages. Coupled with a robust comprehension of digital security fundamentals, such linguistic awareness can act as the foundation for more resilient information ecosystems.

As we move forward, it is vital for scholars, security experts, and citizens to remain vigilant. By fostering critical analysis skills and staying informed about emerging threats – both technical and communicative – individuals can better recognize and counter the array of challenges that exploit vulnerabilities in language, technology, and cognition. Ultimately, understanding the specificity of these threats within the English-speaking sphere is a crucial step toward building a more secure and transparent global information landscape.

2. The role of the English teacher in developing students’ critical thinking and information evaluation skills

Over the past few decades, the field of foreign language teaching has undergone a radical transformation. Traditional methods primarily emphasized memorizing grammatical structures and vocabulary lists, often relegating students to a passive role in the classroom. Rote learning, while useful to a certain extent for building basic linguistic competence, does not necessarily foster the ability to navigate and evaluate complex ideas – a critical need in today’s rapidly changing information landscape.

More recent approaches have shifted from these passive techniques towards a student-centred paradigm, wherein the development of communicative competence intersects with higher-order thinking skills. Instead of treating language learning as an isolated set of structures to be internalized, modern curricula encourage learners to use language as a vehicle for analysis, debate, and self-expression. Within this context, critical thinking emerges as a cornerstone of classroom practice. Students are prompted not only to understand the language but also to engage with the underlying meanings, cultural nuances, and broader contexts in which the language is embedded.

Recent literature demonstrates a growing consensus regarding the pivotal role of English teachers in nurturing learners’ critical thinking and information evaluation abilities. One foundational strand of research appears in Hobbs’s work in the *Journal of Media*

Literacy Education, where she underscores how language instructors can guide students to decode, interpret, and critique multimedia content. Similarly, Kot's et al. (Kot, 2024) meta-analysis in *Science and Education in the Third Millennium* systematically reviews classroom interventions that enhance English as a Foreign Language (EFL) learners' capacity for analytical reading and writing, highlighting strategies such as debates, source evaluation, and problem-based projects. Complementing these studies, Cummins (Cummins, 2020) in the *Journal of Language, Identity, and Education* explores how teachers can foster "language transfer" in multilingual settings, thereby encouraging deeper engagement with texts and sharper awareness of bias across linguistic boundaries.

Despite these significant contributions, gaps remain regarding how precisely to implement critical thinking and information evaluation training in high-stakes contexts – particularly relevant to Ukrainian educators grappling with the effects of the current war. Although Hobbs and Kot detail classroom frameworks applicable to diverse cultural settings, they tend not to address the profound psychological and logistical disruptions encountered in conflict zones. Additionally, UNESCO provides universal guidelines (UNESCO, 2022) but does not specifically cater to the difficulties of teaching critical thinking when fundamental safety and resources are often in question.

Hence, the present study builds upon these scholarly foundations by concentrating on the urgent realities of modern Ukraine. While acknowledging the accomplishments of prior research in clarifying the theoretical underpinnings of critical pedagogy, this article focuses on tailoring and testing practical activities – e.g., analysis of real-time newscasts, cross-checking war-related social media posts – that directly respond to the heightened disinformation threats facing Ukrainian students today. This approach aims to address the previously unsolved parts of the problem, namely how to design, adapt, and evaluate critical thinking pedagogies under conditions of persistent conflict and pervasive media manipulation. Ultimately, the intention is to contribute empirical insights and adaptable strategies that reinforce both linguistic competence and a fortified skill set for independent, critical inquiry.

English language curricula in many educational systems now explicitly incorporate objectives that go beyond basic communication skills. Teachers are expected to design activities that challenge learners to reflect, question, and synthesize information. For instance, learners might read news articles, evaluate the credibility of online sources, or compare differing opinions within a text. By weaving these tasks into lesson plans, educators empower students to develop a more nuanced understanding of the language. This dual focus – on communicative ability and on higher-order thinking – recognizes that language proficiency is not merely an end in itself but rather a tool for critical engagement with the wider world.

Critical thinking: concepts and methods of development

Critical thinking can be defined as the active, disciplined process of conceptualizing, analysing, synthesizing, and evaluating information in order to form a judgement. It involves several interrelated cognitive skills:

- a) analysis – breaking down complex ideas into smaller, more manageable components.
- b) synthesis – combining disparate pieces of information to form new insights or perspectives.

- c) evaluation – assessing the credibility, relevance, and logic of information or arguments.
- d) interpretation – understanding the nuanced meaning of data, texts, or other forms of information.

Critical thinking is widely viewed as a foundational cognitive skill that underpins effective problem solving, decision making, and intellectual inquiry across multiple domains. While it is often described in various ways, most definitions emphasize the capacity to reason objectively and reflectively, systematically examine assumptions, and weigh evidence from multiple perspectives before drawing conclusions. According to leading scholars (*Facione, 2011*), (*Halpern, 2013*), critical thinking comprises core skills such as interpretation, analysis, inference, self-regulation, and evaluation. These skills work together to help individuals identify potential biases – both external and internal – recognize logical fallacies, and question the validity of information sources.

In practical terms, cultivating critical thinking goes beyond mere memorization or passive intake of content. Rather, it involves active engagement with ideas and data: one must challenge initial perceptions, and remain open to alternative viewpoints or hypotheses. This process is iterative and dynamic, requiring an ongoing commitment to intellectual humility and rigorous standards of proof. In modern contexts shaped by rapid technological change and an overabundance of information, critical thinking has become (*Nykyporets, 2024*) an indispensable tool for navigating misinformation and conflicting narratives. As students encounter increasingly complex social, political, and economic challenges, the ability to parse data critically and arrive at well-grounded conclusions empowers them to make informed choices that resonate with ethical and evidence-based principles.

In the context of language learning, these components become especially meaningful. Students often encounter (*Nykyporets, 2023*) texts and dialogues that present differing opinions or require interpretation beyond face-value comprehension. By honing critical thinking abilities, learners become more adept at spotting subtleties in tone, identifying potential bias, or discerning cultural underpinnings in English-language materials.

Methods and techniques for developing critical thinking in language learning

A variety of pedagogical strategies can be integrated into the English language classroom to cultivate critical thinking.

a) Socratic questioning

Instructors prompt students with carefully structured questions that elicit deeper thought. Instead of merely asking, “What does this word mean?” a Socratic question might be, “Why do you think the author chose this particular term to describe the event?” Such questions encourage learners to consider the connotations, context, and implications of language choices, thus moving beyond surface-level understanding.

b) debates

Classroom debates in English offer an excellent way to practice not only speaking and listening skills but also analytical thinking. Students must gather evidence, construct coherent arguments, and critically evaluate opposing viewpoints. In the process, they gain confidence in articulating their thoughts while being exposed to diverse perspectives.

c) case studies

Case studies drawn from real-life scenarios or historical events encourage learners to analyse situations in-depth. Students read and discuss authentic materials, form hypotheses,

and propose potential solutions, all in English. This method brings together textual analysis, critical reflection, and problem-solving, allowing students to see language use in meaningful, context-rich environments.

By incorporating these techniques systematically, teachers can create an interactive classroom atmosphere where students learn to question assumptions, draw reasoned conclusions, and express their viewpoints with clarity and nuance.

The importance of information evaluation skills in the context of information noise and disinformation

In an age characterized by rapid digital communication, students face a barrage of information, some of which may be misleading, biased, or outright false. This information noise becomes more complicated when navigating English-language media and social platforms, where the global audience and diverse sources multiply the volume of content. As a result, learners who consume or produce content in English must develop the capacity to discern reliable evidence from mere speculation and to recognize factual reporting as opposed to manipulative messaging.

Information evaluation, therefore, emerges as a key competence. It requires the ability to cross-check data, understand context, and weigh the credibility of various sources. English teachers, tasked with guiding students in reading and interpreting authentic texts, are uniquely positioned to instil a habit of critical examination. By introducing students to different forms of media – ranging from reputable news outlets to user-generated content on social media platforms – teachers can highlight how to question authenticity, look for corroboration, and identify indicators of potential bias.

Such an approach fosters digital literacy by encouraging learners to engage actively with online content rather than passively consuming headlines or social media posts. It also promotes a questioning mindset, prompting students to compare varied perspectives before arriving at conclusions about events or issues. In regions affected by conflict, such as modern Ukraine, the ability to sift through potentially manipulated or misleading narratives gains particular urgency. By practising information evaluation in the classroom, students can develop resilience against propaganda and develop a stronger sense of personal responsibility for what they share online. Teachers can design group tasks where learners collaborate to verify news stories, researching original sources or consulting fact-checking platforms. Over time, this collective exercise trains them to apply similar scrutiny in their personal use of digital media, helping prevent the rapid spread of unverified claims. Analysing rhetorical devices and persuasive language can further empower students to spot manipulative tactics, whether in political statements, advertisements, or sensational headlines. Teachers might also encourage learners to reflect on their emotional reactions, distinguishing between reasoned judgement and impulsive, fear-based responses. Such self-awareness reinforces the habit of stepping back and evaluating the motives behind every message. Ultimately, strengthening information evaluation skills is a cornerstone of developing responsible, globally minded citizens who can navigate today's challenging information landscape with discernment and integrity.

The expanded involvement of technology in everyday life has made verifying the origin of online materials both more necessary and more complex. Students who engage actively in fact-checking, paraphrasing, and contextualising sources sharpen not only their English language abilities but also their critical faculties. By learning to recognise loaded

language and oversimplifications, they can better judge the reliability and intent of messages circulating in social media ecosystems. In the case of Ukraine, where narratives around the ongoing conflict can be distorted or misrepresented, the cultivation of these skills has far-reaching implications for civic engagement and national security. Educational institutions, therefore, bear a profound responsibility to foster an academic environment that champions evidence-based analysis and open-minded dialogue. Incorporating interactive digital tools – such as online research databases, collaborative annotation software, and multimedia platforms – can amplify students’ capacity to discern credible information. Teachers may also collaborate with librarians or media experts, inviting them to run workshops that simulate real-world challenges in evaluating conflicting data streams. These initiatives help students appreciate the complexity of global events, reinforcing the importance of thorough investigation over superficial judgment. Building these competences early prepares learners for participation in an increasingly interconnected society, where the line between truth and misinformation can often seem blurred. Underpinning these efforts must be a collective commitment to academic integrity, empathy, and a shared pursuit of genuine understanding, values that become indispensable in times of crisis.

Methods and tools for checking sources and using authoritative resources

1. Source triangulation

One of the most effective strategies for confirming the credibility of information is to cross-reference multiple sources. An English lesson might involve students reading a news article from a major international publication, then comparing it with reports from local outlets or specialized research organizations to see if the facts align or if differing perspectives emerge.

2. Fact-checking websites

Encouraging students to use established fact-checking platforms, such as *PolitiFact* or *Snopes*, builds awareness of how to verify or debunk circulating claims. These platforms often illustrate step-by-step how their teams arrive at their verdicts, providing insights into the standards of evidence-based verification.

3. Digital literacy tools

Browser extensions and online tools (e.g., reverse image search) allow students to investigate the origin of images or identify manipulated visuals. Incorporating such tools in classroom activities helps students become more independent in their pursuit of reliable knowledge, while simultaneously enhancing their English vocabulary related to technology and media literacy.

By learning these skills, students develop a systematic approach to navigating the information-rich environment – skill set that not only boosts their English proficiency but also prepares them to be thoughtful, informed global citizens. Through regular practice with authentic materials and fact-checking exercises, they become increasingly adept at discerning credible sources from manipulative propaganda.

Pedagogical techniques for English language teachers. Integration of case studies from English-language sources

A powerful way to fuse language instruction with critical thinking and information evaluation is through the use of authentic case studies. For example, a teacher might select a recent event reported in English-language newspapers, compile several articles offering different viewpoints, and then guide students through a structured analysis. Students could

evaluate the credibility of each source, identify the journalists' or authors' potential biases, and practice synthesizing information into a coherent summary or opinion piece. This method simulates real-world information processing, showing learners how language proficiency and critical analysis intertwine.

The role of project tasks for research and analysis

Extended projects can (*Nykyporets, 2023*) further enhance students' engagement and skill development. In such assignments, learners may be tasked with researching a particular topic – such as environmental policy, cultural practices, or technological innovations – in English-language articles, journals, and websites. Over the course of several weeks, students compile data, keep track of how they assessed the reliability of each source, and ultimately present their findings in oral or written form. The process requires them to practice (*Nykyporets, 2021*) note-taking, source evaluation, and argumentation in English, thereby reinforcing both linguistic competence and analytical rigor.

The use of role-play to practice critical information analysis

Role-play activities offer students a safe yet dynamic setting to exercise creative thinking and language production. A teacher might devise a scenario where disinformation circulates in a fictional community, and learners take on roles such as concerned citizens, journalists, or fact-checkers. Each group is tasked with either spreading or debunking misinformation, compelling students to adapt their use of English in real-time while applying the critical thinking and evaluation techniques learned in class. In this context, language teaching transcends the pages of a textbook: students build practical understanding of how English is used in discourse around truth, accuracy, and manipulation.

In all, the role of the English teacher extends far beyond imparting linguistic knowledge. By deliberately incorporating critical thinking and information evaluation into language instruction, teachers serve as architects of a “protective filter” for their students. This filter equips learners with the capacity to question and verify information, assess diverse viewpoints, and communicate their own perspectives with clarity and discernment – all essential skills in the modern world.

Through the use of targeted pedagogical techniques – Socratic questioning, debates, case studies, and role-plays – educators can foster an environment that challenges students to refine both their English proficiency and their cognitive agility. These efforts contribute (*Nykyporets, 2023*) to shaping informed, proactive individuals capable of identifying manipulation and fake news in the vast English-language information sphere.

This underscores a seamless connection with the next section of our discourse, which will delve deeper into the practice of using authentic materials. By linking theory with real-world applications, we reinforce the premise that English language teaching is not solely about grammar or vocabulary; it is an active, multifaceted process that prepares learners to navigate the complex, often cluttered, global media landscape.

3. Using authentic English-language materials to develop information literacy.

Authentic materials: definition and advantages

The concept of “authentic materials” in foreign language teaching has expanded significantly in recent years, particularly with the advent of digital media. These materials are defined as texts, audio recordings, videos, or any other forms of language content created by and for native speakers, without the primary intention of language learning. They include – but are not limited to – news articles, blogs, speeches, podcasts, vlogs and social media

posts. Their central characteristic is that they reflect genuine usage of the language in real-world contexts, thereby introducing learners to natural discourse patterns, cultural nuances, and contemporary issues.

From the vantage point of a Ukrainian linguist, especially amid the ongoing Russian aggression in Ukraine, harnessing authentic English-language materials acquires greater importance. Access to reliable information sources has never been more critical, as disinformation campaigns – many of which spill over into the English-speaking global media – significantly impact public perception of the conflict. Integrating authentic materials into the curriculum empowers students to become active information consumers, simultaneously advancing their language skills and their resilience against manipulation. Additionally, exposing learners to primary sources from international news outlets fosters a more direct understanding of how global opinion and policy can shape local realities. This heightened language proficiency, combined with enhanced critical awareness, also enables students to more effectively communicate Ukraine's perspective to an international audience. In a broader sense, these educational practices contribute to reinforcing national resilience and promoting a more balanced global discourse about ongoing events.

Advantages of using authentic materials to develop language competence

1. Rich vocabulary. Authentic materials introduce learners to topical, domain-specific vocabulary that textbooks may not yet include, ranging from political discourse to technology jargon. In the context of modern Ukraine, for instance, reports on the war often contain specialized terminology, including terms pertaining to military strategy, diplomacy, humanitarian aid, and sanctions.
2. Cultural context and realism. Textbooks frequently sanitize or oversimplify language to fit a pre-structured syllabus. Authentic resources, on the other hand, showcase regional dialects, cultural references, and even slang – essential elements for understanding the real, living language.
3. Relevance and engagement. When learning materials connect directly to current global or local events, student motivation tends to increase. Learners see the practical applications of improving their English proficiency, such as reading international news, engaging in global discussions on social media, or communicating with volunteers.
4. Analytical and critical skills. The authenticity of the sources compels students to adapt to varied writing styles, viewpoints, and tones. By navigating these complexities in real time, they cultivate advanced reading comprehension and critical thinking capacities, indispensable for parsing propaganda and manipulative discourse.

Types of English-language sources and their thematic specificity

Authentic materials span a wide range of themes and genres. They can include everything from newspaper articles, radio broadcasts, and video interviews to social media posts and user-generated content, providing learners with exposure to real-world language use and contextualized cultural references. Learners can explore mainstream international news outlets, specialized investigative reports, niche blogs focusing on cultural or scientific topics, and even official statements from foreign governments of different countries. When confronting the realities of the Russian-Ukrainian war, for instance, reading reports from think tanks or official statements made by international organizations can provide deeper

insight into how global media interprets the conflict. Each source category offers unique language features – formal, conversational, or even anecdotal – thus preparing students for the variety of registers they might encounter in real life every day.

Mass media, social media, and analytical resources: forms and methods of working with authentic materials

Reputable international news platforms such as *BBC*, *CNN*, *The Guardian*, and *The New York Times* often have broad coverage of global events, including Russia’s aggression against Ukraine. Additionally, numerous specialized outlets focus on military analysis, political commentary, or economic research. When selecting articles or videos for classroom activities, teachers can compare how these different sources present the same event, prompting students to analyse not just the language itself but also potential biases and framing tactics. In contrast, local and regional publications may provide unique perspectives, yet may also reflect specific cultural or political leanings. By cross-checking narratives from both global and niche media outlets, students gain a more comprehensive understanding of how events are reported and contextualized.

Social media usage has skyrocketed in Ukraine in recent years, serving both as a platform for civic engagement and an arena for disinformation campaigns. *X(Twitter)*’s character limit encourages succinct, sometimes emotionally charged statements, while *Facebook* groups or *Telegram* channels can foster closer-knit communities around specific topics – be they humanitarian aid updates or pro-Ukrainian activist groups. Meanwhile, *LinkedIn* offers a more professional, formal register. Each platform carries its unique “content features and risks”.

Table 4.

Key content features of social media and their potential risks

	Content feature	Description	Risk
1.	Virality	False information can spread quickly	Rapid circulation of misleading content can reach large audiences before it can be fact-checked or corrected.
2.	Echo chambers	Users might only see content that aligns with their existing viewpoints	Reinforcement of existing biases, leading to polarization and reduced exposure to diverse perspectives.
3.	Linguistic variation	Posts can be highly informal or riddled with abbreviations, hashtags, and emoticons	Risk of misinterpretation or ambiguity, making it harder to assess credibility and detect manipulative messaging.

Source: created by authors.

Analytical resources: think tanks, official government reports, and scientific journals

English-language think tanks, such as *Chatham House* or the *RAND Corporation*, often release detailed reports on military conflicts, international relations, or global security trends. Government websites issue official statements and documents, providing language learners with insight into formal diplomatic and legal discourse. Scientific journals, albeit more specialized, can be relevant for advanced students or those interested in the technical underpinnings of modern warfare (e.g., cybersecurity, drone technology). By engaging with these materials, students practice discerning objective data-driven language from opinion or speculation. Moreover, analysing these sources can deepen learners’ understanding of the

institutional frameworks and rhetorical strategies used to present sensitive information. This expanded skill set enhances their readiness for professional and academic pursuits where data interpretation and evidence-based arguments are crucial.

Forms and methods of working with authentic materials

- 1. Comparative reading. Students read multiple articles on the same event to recognize differences in style, word choice, and framing.
- 2. Listening comprehension. Short news broadcasts or podcasts help train students to identify speakers’ intonation and detect manipulative rhetoric.
- 3. Task-based projects. Learners may create a mini research report or presentation after consulting various authentic English-language sources, reflecting on their methods for verifying credibility.

Developing the ability to recognize unreliable sources and enhance language skills

Table 5.

Pedagogical strategies for enhancing students’ critical thinking and information evaluation skills

		Objective	Process	Outcome
1	Reading and analysing articles or social media posts	Strengthen students’ ability to identify potential red flags (e.g., lack of credible references, exaggerated or emotionally charged language, inconsistent data)	Encourage learners to ask who the author is, what their background might be, and whether other reputable outlets corroborate the story.	Enhanced reading comprehension and critical literacy, both crucial for navigating disinformation prevalent in war contexts.
2	Listening to and watching podcasts/videos	Develop “sensitivity” to intonation shifts that might reveal sarcasm, fearmongering, or subtle manipulative accents.	Students watch or listen to a short podcast on current events in Ukraine, pausing to discuss tone, body language (in video), and argumentation techniques.	Improved listening skills and heightened awareness of rhetorical devices and emotional cues.
3	Writing (reflection, review, critical analysis)	Hone the ability to articulate reasoned arguments, indicate agreement or disagreement, and present counter-evidence.	Assign reflective essays or responses to English-language articles. Students must cite sources, state arguments, and propose solutions or counterarguments.	Reinforced writing fluency alongside logical structuring of viewpoints, mirroring the demands of university-level course-work or international communication.
4	Developing information literacy: technologies and tools	Familiarize students with practical methodologies for cross-checking facts and authenticating images or data.	Demonstrate reverse image search (e.g., Google Images, TinEye), official press releases, or publicly available data repositories.	Cultivation of digitally-savvy learners who can confidently filter truths from falsehoods – a particularly urgent skill given the war-related propaganda in multiple languages.

Source: created by authors

Interactive platforms and practical cases for classroom and self-study

Websites like *FactCheck.org*, *PolitiFact*, and *Snopes* provide invaluable lesson content. Teachers can assign tasks in which students research a claim about the war in Ukraine (e.g., a viral video allegedly showing events on the frontline), compare it to verified sources, and present their findings. This repetitive process of “analyse, compare, conclude” builds methodological rigor into the learning experience. Furthermore, these assignments encourage students to adopt a proactive stance in verifying information, reinforcing their capacity to act responsibly and conscientiously in digital spaces.

Social media analysis tools

Platforms such as *CrowdTangle* or *TweetDeck* help track hashtags, influencer accounts, and content circulation patterns. Students can analyse how certain narratives gain traction, noting rhetorical patterns or bots amplifying disinformation. This not only strengthens language comprehension but also expands their digital literacy. In turn, they gain critical insights into the mechanics behind modern information ecosystems.

Online courses and thematic WebQuest tasks

Coursera/edX. Free or low-cost courses on subjects such as media literacy, global politics, or journalism ethics, often conducted in English. Students can practice specialized vocabulary and broaden their worldview.

Thematic WebQuest. Learners follow a structured online inquiry that culminates in a project or presentation. For instance, a *WebQuest* on “Reliable reporting on the Donbas situation” guides students through official statements, NGO sites, and news outlets, prompting them to form evidence-based conclusions.

Practical cases

Case 1. Comparing news outlets on civilian evacuations

Students examine *BBC* and *CNN* reports on the urgent evacuation of civilians in a specific Ukrainian town, carefully cross-referencing relevant facts with a credible local Ukrainian news platform. They meticulously document significant discrepancies or omissions and openly discuss possible underlying reasons (e.g., editorial focus, deadlines, biases, political pressures).

Case 2. Social media misinformation via *Telegram*

The teacher selects a viral *Telegram* post claiming an “urgent military update.” Students use verification steps: checking official government *Telegram* channels, verifying images via reverse search, and reviewing reputable Western sources. The exercise highlights potential manipulative language and the importance of cross-referencing.

Analysing examples of disinformation and manipulative materials in the English-language environment

Given the Russian-Ukrainian war, instances of outright fabrications and subtle manipulations abound in the international media landscape. Below are three illustrative examples that can be examined collectively.

Following the analysis, students prepare mini-presentations or mini-research projects on fact-checking methodologies. Presentations might include their step-by-step approach, discoveries, and final assessments of the claims’ veracity. By sharing their findings with peers, learners also refine public speaking skills and reinforce collaborative learning dynamics.

Table 6.

Examples of fabrications and manipulations

		Type	Real issue	Activity
1.	Fake military videos	Clips allegedly showing Ukrainian forces in conflict situations.	Footage from a completely different region or even a different year, mislabelled to skew public perception.	Students check the video's metadata, compare timestamps, or use specialized fact-checking communities (e.g., Bellingcat)
2.	Biased "expert" commentary	An individual touted as a military or geopolitical expert writing op-eds in English-language newspapers	The "expert" may lack credible credentials or may have ties to lobbying groups	Class discussion on evaluating an author's background, cross-referencing professional affiliations or publications
3.	Sensational headlines in clickbait websites	Overly dramatic headlines that claim immediate catastrophes or breakthroughs	Exaggeration or manipulation to capture more clicks, often referencing the war out of context	Students analyse the textual structure, rhetorical style, and credibility signals (or lack thereof), leading to a mini-research project on truthfulness versus sensationalism

Source: created by authors

This collaborative environment fosters reflection on personal strategies for media consumption. Students become more confident in identifying manipulative materials and distinguishing legitimate journalism from propaganda. Feedback sessions can highlight best practices – such as verifying multiple sources, paying close attention to editorial disclaimers, and maintaining a cautious attitude towards sensational or “too good to be true” narratives.

In sum, employing authentic English-language materials in a linguistically oriented curriculum is more than just a strategy for vocabulary expansion or fluency improvement – it is a foundational approach that shapes information literacy. Learners not only become adept at handling the complexities of real-world English but also gain vital skills for identifying and mitigating the impact of disinformation, which is particularly consequential in the Ukrainian context beset by hybrid warfare and propaganda.

Further prospects: integrating these approaches into technical university curricula.

First, interdisciplinary collaboration is crucial: by coordinating with IT departments, educators can enhance students' cyber literacy and fact-checking proficiency. Next, sustained relevance can be achieved (*Nykyporets, 2024*) by developing semester-long projects in which students track the evolution of a major event related to the war, fostering ongoing analytical engagement. Finally, international collaboration is essential: by partnering with educators abroad, instructors can compare classroom experiences and share best practices for integrating authentic materials and disinformation analysis into the curriculum.

By embedding these techniques into language programs across secondary and higher education, we prepare Ukrainian students not only to function effectively in an English-speaking environment but also to serve as informed, critical-minded participants in shaping the future – both for Ukraine and the broader international community.

Summary. In this chapter, we explored how information security in the English-speaking context intertwines with the realities of modern Ukraine, particularly against the backdrop of the Russian-Ukrainian war of aggression. The chapter's structure unfolds in three key segments, each shedding light on theoretical concerns and practical classroom applications.

In the first part, we addressed the main types of contemporary information threats and explained why the English-speaking sphere plays such an influential role. We observed that English has become a global tool not only for legitimate communication but also for the dissemination of disinformation. This context resonates with Ukraine's current struggles, where numerous manipulative narratives – often crafted in or translated into English – aim to shape international perceptions of the conflict.

Building on these insights, the second part turned to the pedagogical dimension. Here, we focused on how English teachers can equip students with critical thinking skills vital for recognizing misinformation. By integrating analytical exercises, debates, and open dialogues into language lessons, educators foster a learning environment in which students practice (*Stepanova, 2024*) evaluating sources and questioning biased content. This emphasis on critical scrutiny directly addresses (*Medvedieva, 2023*) the urgent need for Ukrainians, especially the younger generation, to protect themselves from propaganda and manipulative messaging tied to the ongoing war.

Finally, the third part offered concrete methods and authentic resources for strengthening information literacy in parallel with language proficiency. We examined (*Ibrahimova, 2024*) real-world materials – news articles, podcasts, social media posts – as vehicles for cultivating both linguistic aptitude and evaluative judgment. Interactive tools such as fact-checking websites and social media analysis platforms were showcased to illustrate how learners can verify content before accepting or sharing it. By intertwining theoretical approaches to information security with pragmatic classroom strategies, the chapter highlights an actionable path forward: students empowered to engage critically with English-language content, and thereby contribute to Ukraine's broader resistance against disinformation. At the same time, these strategies can be expanded beyond the classroom, helping to cultivate a society-wide culture of media literacy and civic engagement.

By promoting cross-cultural dialogues and demonstrating the effectiveness of fact-checking tools, educators and learners together become catalysts for more ethical and transparent communication across diverse digital platforms. In doing so, they contribute to a globally networked defence against manipulative narratives that thrive on public ignorance or misunderstanding. As language learners attain a solid grasp of media literacy, they become empowered to engage in complex international discourses with greater confidence and discernment. Ultimately, the synergy between advanced language competence and heightened critical awareness stands as a vital pillar of Ukraine's ongoing resilience, reinforcing both national sovereignty and the democratic values that underpin it. This synergy is especially salient in an era of swiftly evolving media landscapes, where misinformation can spread faster than traditional fact-checking processes. By incorporating real-life case studies, educators show students how fabricated narratives erode social cohesion and trust in public institutions. Over time, such classroom approaches help normalize scepticism and thorough verification, turning critical analysis into a habitual practice rather than an isolated exercise.

Furthermore, students acquire the ability to identify the structural elements of deceptive materials, from sensational headlines to misleading statistical presentations. These skills not only benefit them academically but also inform their civic engagement and responsible behaviour online. The next step is expanding these efforts through professional development programs that give teachers the confidence and tools to seamlessly incorporate authentic materials and media literacy into their lessons. When teachers have robust institutional support, they can adapt methods to a range of language abilities and age groups, ensuring more inclusive access to these crucial skills. Beyond formal education, well-designed community workshops and public awareness campaigns can amplify the impact of media literacy initiatives. Such collective strategies bring Ukraine ever closer to achieving “information autonomy,” wherein citizens can independently discern the truth and remain vigilant against external manipulation.

References:

- Baltutis D., Teubner T., Adam M. T. P. A typology of cybersecurity behavior among knowledge workers. *Computers & Security*. 2024. Vol. 140. Art. 103741. DOI: <https://doi.org/10.1016/j.cose.2024.103741>.
- Wardle C., Derakhshan H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking. *Council of Europe*, 2017. URL: <https://surl.li/xbarbc> (Accessed on: 11.02.2025).
- Hobbs R., Moen M., Tang R., Steager P. Measuring the implementation of media literacy instructional practices in schools: community stakeholder perspectives. *Learning, Media and Technology*. 2022. DOI: <https://doi.org/10.1080/17439884.2022.2151621>.
- Li M., Murphy P. K., Wang J., Mason L. H., Firetto C. M., Wei L., Chung K. S. Promoting reading comprehension and critical-analytic thinking: A comparison of three approaches with fourth and fifth graders. *Contemporary Educational Psychology*. 2016. Vol. 46. P. 101-115. DOI: <https://doi.org/10.1016/j.cedpsych.2016.05.002>.
- Cristiano F., Kurowska X., Stevens T., Hurel L. M., Fouad N. S., Dunn Cavelti M., Broeders D., Liebetrau T., Shires J. Cybersecurity and the Politics of Knowledge Production: Towards a Reflexive Practice. *Journal of Cyber Policy*. 2023. Vol. 8, No. 3. P. 331–364. DOI: <https://doi.org/10.1080/23738871.2023.2287687>.
- Chinn C. A., Barzilai S., Duncan R. G. Education for a “Post-Truth” World: New Directions for Research and Practice. *Educational Researcher*. 2021. Vol. 50, No. 1. P. 51-60. DOI: <https://doi.org/10.3102/0013189X20940683>.
- Nurturing Trust: A Media and Information Literacy Imperative. Global Media and Information Literacy Week, 24-31 October 2022. UNESCO. URL: <https://tinyurl.com/ytmu9uqb>. (Accessed on: 11.02.2025).
- Brown H., Lee K., Mireshghallah F., Shokri R., Tramèr F. What Does it Mean for a Language Model to Preserve Privacy? In 2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT '22), June 21–24, 2022, Seoul, Republic of Korea. ACM, New York, NY, USA. 13 p. DOI: <https://doi.org/10.1145/>.
- Jowett G. S., O'Donnell V. Propaganda & Persuasion. 6th ed. University of Houston, Montana State University. Thousand Oaks, CA: SAGE Publications, Inc., 2015. URL: <https://surl.li/sfboyu> (Accessed on: 12.02.2025).
- Betancourt Á., Guasch M., Ferré P. What distinguishes emotion-label words from emotion-laden words? The characterization of affective meaning from a multi-componential conception of emotions. *Front. Psychol*. 2024. Vol. 15. Art. 1308421. DOI: <https://doi.org/10.3389/fpsyg.2024.1308421>.
- Kot S. O., Nykyporets S. S. Utilization of artificial intelligence in enhancing English language proficiency in tertiary education. *Science and Education in the Third Millennium: Information Technology, Education, Law, Psychology, Social Sphere, Management : International collective monograph*. Institute of Public Administration Affairs, Lublin, Polska, 2024. Chap. 10. P. 250-274. DOI: <https://doi.org/10.5281/zenodo.11279390>.

- Cummins J. Current research on language transfer. Hamburg Studies on Linguistic Diversity. 2013. Book chapter. DOI: <https://doi.org/10.1075/hsld.1.15cum>.
- Facione P. A. Critical thinking: What it is and why it counts. Research Report. Millbrae, CA: The California Academic Press, 2011. URL: <https://surl.li/wfpcwx> (Accessed on: 14.02.2025).
- Halpern D., Gibbs J. Social Media as a Catalyst for Online Deliberation? Exploring the Affordances of Facebook and YouTube for Political Expression. *Computers in Human Behavior*. 2013. Vol. 29. P. 1159-1168. DOI: <http://dx.doi.org/10.1016/j.chb.2012.10.008>. URL: <https://surl.li/qozqqf>
- Nykyporets S. S., Melnyk O. D., Ibrahimova L. V., Hadaichuk N. M., Derun V. H. Advancing critical thinking skills among higher education students through English language instruction: contemporary approaches and strategies. *Prospects and innovations of science. Series "Pedagogy"*. 2024. № 1(35). Pp. 34-45. DOI: [https://doi.org/10.52058/2786-4952-2024-1\(35\)-34-45](https://doi.org/10.52058/2786-4952-2024-1(35)-34-45).
- Nykyporets S. S., Melnyk O. D., Ibrahimova L. V., Boiko Yu. V., Kukharchuk H. V. Fostering critical thinking in technical university students in foreign language classes: strategies and approaches for cultivating analytical proficiency. *Bulletin of Science and Education. Series "Pedagogy"*. 2023. № 8(14). C. 344-360. DOI: [https://doi.org/10.52058/2786-6165-2023-8\(14\)-344-360](https://doi.org/10.52058/2786-6165-2023-8(14)-344-360).
- Nykyporets S. Utilizing a case study approach to foster critical thinking in foreign language teaching for masters in power engineering. *Collection of scientific papers «ΛΟΓΟΣ»* with Proceedings of the III International Scientific and Practical Conference, Cambridge, August 18, 2023. P. 191-196. DOI: <https://doi.org/10.36074/logos-18.08.2023.54>.
- Nykyporets S.S. Interactive technologies in foreign language lessons as a way of critical thinking formation for students of non-linguistic universities. *International scientific and practical conference «Philological sciences, intercultural communication and translation studies: theoretical and practical aspects»: conference proceedings*, February 26-27, 2021. Venice: Izdevnieciba «Baltija Publishing», 2021. 184 pages, pp. 156-160. DOI: <https://doi.org/10.30525/978-9934-26-039-1-97>.
- Nykyporets S. S., Stepanova I., Hadaichuk N. Tools and techniques to develop higher order thinking skills in students of non-linguistic technical universities of Ukraine during online learning. *Norwegian Journal of Development of the International Science*. 2023. № 1117. P. 44-49. DOI: <https://doi.org/10.5281/zenodo.8385809>.
- Nykyporets S. Utilizing a case study approach to foster critical thinking in foreign language teaching for masters in power engineering. *Collection of scientific papers «ΛΟΓΟΣ»* with Proceedings of the III International Scientific and Practical Conference, Cambridge, August 18, 2023. P. 191-196. DOI: <https://doi.org/10.36074/logos-18.08.2023.54>.
- Nykyporets S. S., Kot S. O., Herasymenko N. V., Chopliak V. V., Kukharchuk H. V. Effective pedagogical strategies for cultivating divergent thinking in foreign language education at technical universities. *Society and national interests. Series «Education/Pedagogy»*. 2024. № 6(6). Pp. 23-35. DOI: [https://doi.org/10.52058/3041-1572-2024-6\(6\)-23-36](https://doi.org/10.52058/3041-1572-2024-6(6)-23-36).
- Nykyporets S. S., Kot S. O., Boiko Yu. V., Melnyk M. B., Chopliak V. V. Advanced integration of virtual information environments (VIEs) in contemporary educational methodologies. *Society and national interests. Series «Education/Pedagogy»*. 2024. No. 4(4). Pp. 139–154. [https://doi.org/10.52058/3041-1572-2024-4\(4\)-139-154](https://doi.org/10.52058/3041-1572-2024-4(4)-139-154).
- Nykyporets S. S., Kot S. O., Hadaichuk N. M., Melnyk M. B., Boiko Y. V. Innovative pedagogical strategies for utilizing online platforms in foreign language acquisition. *Current issues in modern science. Series «Pedagogy»*. 2024. No. 5(23). P. 730–743. DOI: [https://doi.org/10.52058/2786-6300-2024-5\(23\)-730-743](https://doi.org/10.52058/2786-6300-2024-5(23)-730-743).
- Stepanova I. S., Nykyporets S. S., Hadaichuk N. M. Digital transformation of language education at a technical university: challenges, opportunities and prospects for cooperation with European partners. *Цифровізація як інструмент забезпечення якості надання освітніх послуг з урахуванням європейського досвіду: колективна монографія / за ред. А. В. Череп, І. М. Дашко, Ю. О. Огренич, О. Г. Череп. Запоріжжя : видавець ФОП Мокшанов В. В., 2024. 300 с. С. 36-85. <https://doi.org/10.5281/zenodo.14258696>.*
- Medvedieva S. O., Stepanova I. S., Nykyporets S. S., Ibrahimova L. V. The application of a neuropedagogical approach while teaching English to students of higher educational establishments.

Prospects and innovations of science. Series 'Pedagogy'. 2023. № 8(26). C. 13-24. DOI: [https://doi.org/10.52058/2786-4952-2023-8\(26\)-13-24](https://doi.org/10.52058/2786-4952-2023-8(26)-13-24).

Nykyporets S. S., Boiko Yu. V. Practical tips and interactive learning tools for the work of a foreign language teacher at a technical university in the conditions of blended learning during the full-scale military aggression of Russia against Ukraine. *World trends in the use of interactive technologies in education. International collective monograph.* Intellebence Transportation System And Smart City Institute (ITSSCI). Lima, Peru, 2024. Chap. 14. P. 322-348. DOI: <https://doi.org/10.5281/zenodo.10653715>.

Ibrahimova L., Nykyporets S., Derun V., Herasymenko N. Information and communication technologies as a means of teaching foreign languages in technical higher non-linguistic universities. *Scientific Collection «InterConf».* 2021. № 93. Umeo, Sweden. C. 91-100. DOI: <https://doi.org/10.51582/interconf.21-22.12.2021.010>.

CHAPTER 13.

ECONOMIC SECURITY OF UKRAINE IN THE CONTEXT OF A FULL-SCALE WAR

Yana KOTKO

PhD in Economics, Associate Professor of the Department of Economics and Business,
State Biotechnological University,
(Kharkiv, Ukraine, Alchevskikh str. 44)

kotkoyana@ukr.net

<https://orcid.org/0000-0001-6611-8130>

Abstract. The economic security of the state is an important factor for ensuring the stability and prosperity of the country. Measures to ensure economic security include infrastructure development, investment promotion and business development. In today's globalized world, economic security is becoming a key component of the national security of every country. To this end, it is important to develop effective strategies and mechanisms aimed at protecting national interests, avoiding crises and ensuring continued economic development. This may include various methods, support, and tools. Implementing a mechanism to ensure economic security is crucial for the country's sustainable development. By ensuring economic stability and security, a country can attract investment, create wealth and improve the living standards of its citizens.

Keywords: economic security, mechanism of ensuring, state potential, national economy, sustainable development.

Introduction. Ukraine's economic security is undergoing significant transformations in the context of a full-scale war. Having passed the stage of stabilization and adaptation to a full-scale invasion, the national mechanism for ensuring economic security has gradually begun to transition to a wartime economy. This simultaneously leads to cautiously optimistic directions for economic recovery and creates new challenges and threats to the economic security of our country.

Throughout a full-scale war, emerging challenges and threats to economic security are primarily related to the direct destructive impact of hostilities on economic development. This includes physical destruction of critical assets and economic infrastructure, inability to conduct economic activities in combat zones, missile and drone attacks, lack of skilled labor, and potential increase in macroeconomic imbalances. These factors could significantly impede economic growth and stability in the affected regions.

This is a significant challenge to Ukraine's economic security, as uncertainty about the extent of the damage caused by the war and the possibilities for compensation complicates the process of restoring the country's economic potential in various sectors. The time and financial prospects for recovery may be important factors affecting Ukraine's economic sustainability. To address these challenges, it is important to implement comprehensive strategies and measures aimed at improving the country's economic situation.

Despite the ongoing war, which is affecting economic growth and increasing dependence on external sources of development, the country's economic security has

generally stabilized. This situation emphasizes the challenges the country faces in achieving sustainable economic growth in the context of the conflict and increased external dependence. The economic situation in Ukraine in 2023 and the losses caused by the war did not allow the country to reach the pre-war level of gross domestic product. However, in 2023, there was some economic growth of 5.3%, which exceeded previous forecasts and allowed for a stable situation and reduced risks to economic security after a full-scale invasion.

In order to achieve pre-war levels of real gross domestic product, the national economy needs to have stable economic development and take into account all factors that may affect economic growth. In particular, it is important to have an effective investment policy, develop infrastructure, support business, and create favorable conditions for growth. The IMF can provide additional support and guidance to help achieve economic growth goals. According to the International Monetary Fund's forecasts, in 2027, the level of gross domestic product could be almost 91-92% of the gross domestic product in 2021.

The improvement in the economic situation in 2023 paved the way for an increase in domestic consumer demand. However, the growth rate remains low and is supported mainly by public social spending rather than by a steady increase in household income due to improved economic activity in the country. Much of this funding was provided by international financial assistance from partner countries to support the state budget. Positive changes in employment contributed to a gradual recovery in domestic consumer demand in 2023, with labor demand in Ukraine growing dynamically.

Despite the positive trends, the lack of a predictable scenario for the end of a full-scale war makes it difficult to identify challenges and threats to Ukraine's economic security. One of the new risks is the possibility of blocking or discriminatory restrictions on the free cross-border movement of goods from Ukraine to the EU, which could disrupt trade flows and affect economic stability. An escalation of external instability due to a potential expansion of hostilities could also disrupt supply chains and negatively impact various economic processes in Ukraine and partner countries.

To minimize the risks to Ukraine's economic security, an important task is to maintain macroeconomic stability, preserve a favorable environment for investment, innovation and industrial development, and restore the dynamics of social development, which are key tasks for Ukraine's economic security.

Thus, to improve Ukraine's economic security, it is necessary to improve the anti-corruption system, attract foreign investors, develop exports of goods and services, improve infrastructure, and invest in education and science.

The paradigm of economic security and the peculiarities of its manifestation.

In a full-scale war, it is very important to ensure the economic security of the country. This means protecting national economic interests, maintaining the stability of the financial system, developing production and securing vital resources. An efficient economy helps a country survive in war by providing the necessary resources for the army and the population.

The economic security of the state plays an important role in determining the prospects and pace of socio-economic development. The level of economic security reflects the resilience of the national economy to external challenges and internal threats. Ensuring economic security increases the chances for stable economic development and contributes to improving the quality of life of citizens.

Ensuring economic security is extremely important for the state in the modern world.

This includes various aspects such as protecting economic infrastructure from external threats, ensuring the stability of the financial system, and maintaining competitiveness in the international market.

Research into these issues is indeed relevant, as it allows for timely identification of potential risks and appropriate measures to prevent them. The economic security of the state plays a key role in ensuring the national security and sovereignty of Ukraine. Building an effective economic security system allows timely detection of threats to national economic interests and prevention of damage to the country's socio-economic system as a whole.

The number of researchers and scientific publications on the economic security of the state is indeed constantly growing. This demonstrates the growing interest in this problem and the importance of research in this area. This development contributes to the improvement of scientific knowledge and practical solutions in the field of economic security of the state. The evolution of the formation of economic thought in the field of defining the theoretical foundations of economic security can be studied in the scientific works of Ukrainian scientists, primarily Gbur Z., Krymchak L., Melnyk T., Kozlovsky S. (*Kozlovskiy S., Horun S., Mamashvili L., 2024*). The key issues of economic security in Ukraine are reflected in the works of such scholars as Masliy O., Kivshyk O., Kotelevets M. (*Masliy O., Kivshyk O., Kotelevets M., 2023*).

Other researchers Lipkan A., Romanenko O., Kornienko T. (*Korniienko T., 2022*) consider issues related to the economic and national security of Ukraine, in particular, focusing on the criteria, indicators and methodology for assessing and ensuring economic and national security. These are important aspects that need to be carefully assessed and addressed to ensure the stability and prosperity of the country.

Economic security is closely intertwined with various functional components and their interdependencies, which requires a comprehensive approach to analysis and protection. It is extremely important to take into account the current state and existing challenges in order to formulate effective strategies for strengthening the economic and national security of Ukraine.

The works of Generalov O. (*Generalov O., Romanenko O., 2021*), Pushak Y. (*Pushak Ya., Trushkina N., 2022*), Cherevko I. (*Cherevko I., Fliak Yu., 2024*) reflect the study of the issues of identifying current threats to the economic security of the state, which may include economic crises, corruption, lack of competitiveness, technological threats, which is extremely important for the development of effective strategies and policies in the field of economic security of the state. To ensure the economic security of the state, it is necessary to develop strategies and mechanisms of protection, as well as to cooperate with other countries and international organizations.

Thus, the essence of a country's economic security lies in its ability to protect its economy from various internal and external threats. These threats can range from political instability and corruption to economic crises and natural disasters. Further research on this topic is needed to better understand the challenges and implement effective strategies to protect its economic security. To ensure the long-term stability and prosperity of the nation, it is important to identify and counter these threats proactively (*Kozlovsky S., 2024; Masliy O., 2023*).

National security activities are crucial to Ukraine's future. Understanding and correcting mistakes made in the process of economic reforms is indeed a key aspect of

ensuring stability and prosperity in the country. It is also important to support social development and national identity of citizens (*Kornienko T., 2022*).

Economic security is the state of the economy when it is stable and free from significant risks or threats. The main components of economic security are stable economic growth, low inflation, low unemployment and a stable national currency. Ensuring the economic security of the country includes various mechanisms, such as maintaining a strong and diversified economy, implementing effective fiscal and monetary policies, facilitating trade and investment, and protecting critical infrastructure.

The main challenges to economic security include external factors such as global economic instability, trade wars and economic sanctions, as well as internal factors such as corruption, ineffective government policies and lack of transparency in economic decision-making. In foreign and domestic literature, there are many approaches to interpreting the concept of economic security of the state. Some view it as the ability of the state to maintain stable economic growth and protect its resources from external threats, while others emphasize the importance of having a stable economic system capable of withstanding shocks and shocks. In general, the concept of economic security is complex and multifaceted, and different scholars and experts may have different views on how it should be defined and achieved (Figure 1) (*Generalov O., 2021*).

After analyzing the existing approaches (Figure 1) to defining the economic security of the state, we can conclude that the economic security of the state is a key aspect of ensuring the stability and prosperity of society. To achieve this goal, it is necessary to develop effective strategies and measures aimed at protecting the country's economic interests in the face of a changing international environment and domestic economic challenges. This approach will ensure sustainable economic development, improve the welfare of the population and ensure the national security of the country.

Economic security is the most important aspect of the overall security and stability of a country. Theoretically, it encompasses various components that are important for ensuring the financial well-being and sustainability of the country (Figure 2).

These components (Figure 2) typically include policies and measures aimed at stabilizing the economy, protecting key industries, ensuring a reliable energy supply, maintaining a stable currency, fostering innovation and technological progress, and defending against external threats such as economic espionage or cyberattacks. By understanding and addressing these key elements, a country can enhance its economic security and reduce vulnerabilities that could undermine its prosperity and stability.

The complexity of the existing challenges (Figure 3) faced by the state requires the identification of balanced strategies to address them. These strategies should take into account the interconnection between the issues of national security, socio-economic development and information security of the economic system. Given the current situation in the Ukrainian economy, the problems of economic security and the search for methods and ways to protect the Ukrainian economy are more relevant than ever. It is important that policymakers and stakeholders effectively address these challenges to ensure the stability and growth of Ukraine's economy (*Pushak Y., 2022; Cherevko I., 2024*).

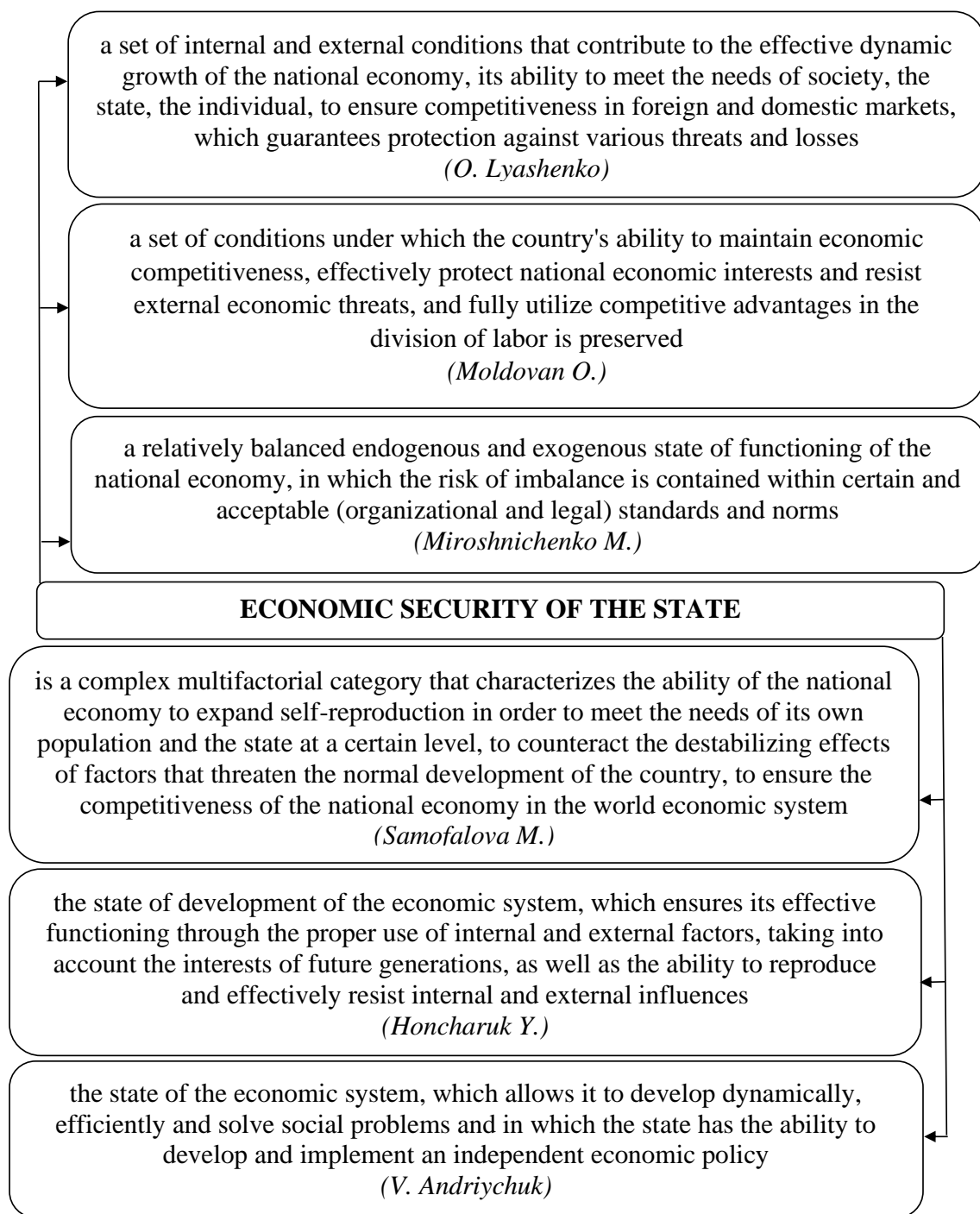


Figure 1. Basic concepts of the concept of «economic security of the state»

Source: author's elaboration based on (Moldovan O., 2021)

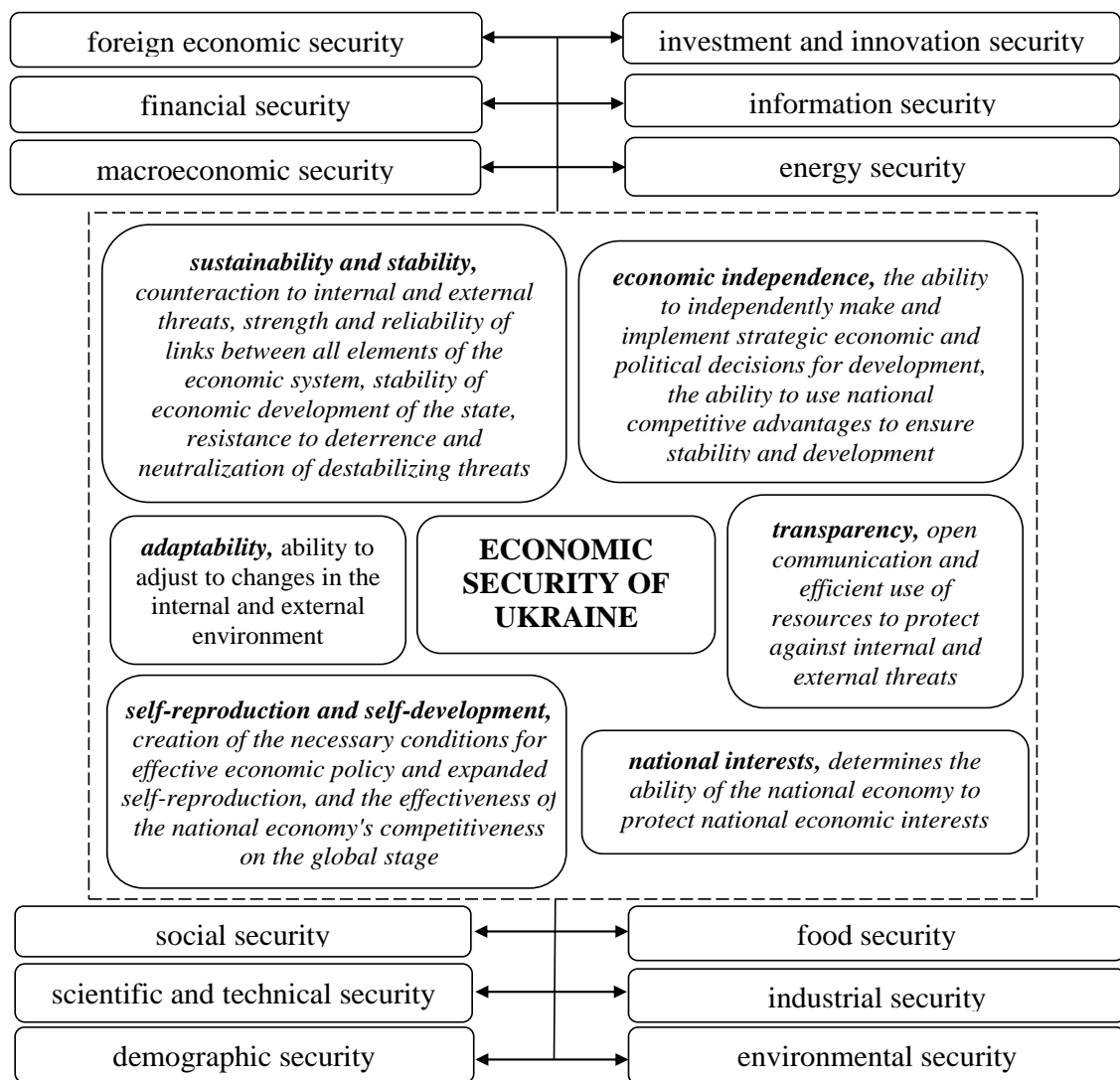


Figure 2. Main components of Ukraine's economic security

Source: developed by the author on the basis of (Moldovan O., 2021)

Today, critical threats to economic security associated with the negative consequences of war are becoming more urgent. These threats include a reduction in labor potential, lack of financial resources, and complications in the ability to quickly restore economic activity in wartime. Risks are also associated with the collapse of industrial and export potential, problems with debt accumulation, and a decrease in investment caused by the war (Lizun M.V., Ozarko K.S., 2023).

The risks that may arise from a growing trade deficit, a loss of Ukraine's export potential due to the destruction of production facilities, difficulties in exports due to problems with transport logistics, an increased focus on raw materials and low-tech exports, and an increase in imports for domestic consumption are currently of concern. It is important to develop strategies and policies to mitigate these risks and ensure the country's sustainable economic development (Table 1) (Dmitrova O.S., Tereshchuk O.D., Karpova K.V., 2023).

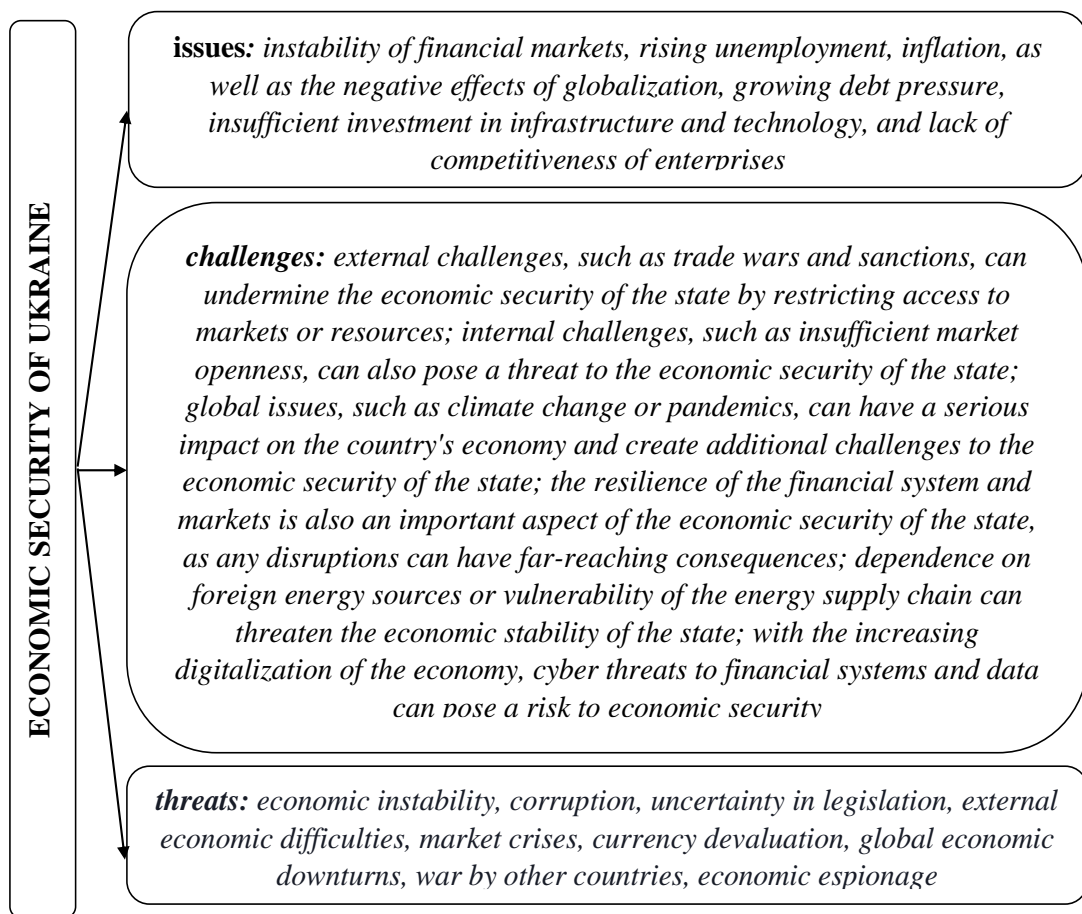


Figure 3. Current challenges to Ukraine's economic security

Source: developed by the author on the basis of (Lizun M.V., Ozarko K.S., 2023)

The sharp economic downturn caused by the restrictions on business activity in the war and the inability to do business in certain regions of the country, such as conflict zones or high-risk areas, is a significant challenge. The prolonged nature of the war creates a constant and difficult to predict threat of new destruction of industrial potential and infrastructure. This threat extends not only to the frontline areas but also to other regions of Ukraine that suffer losses from enemy attacks. The ongoing conflict is creating a serious economic and humanitarian crisis for the country, with far-reaching consequences for its population and industry. In particular, Ukraine's trade balance has deteriorated significantly. In 2022, the negative balance of trade in goods and services increased to almost USD 26 milliards, mainly due to a decline in exports compared to imports and a sharp increase in imports of services. This trend continued in 2023, when the negative balance of trade in goods and services increased to USD 38 milliards.

Analyzing the economic situation, we can conclude that businesses have shown extraordinary resilience and the ability to quickly adapt to difficult conditions. Investment projects aimed at strengthening energy resilience and restoring production are a step forward in the country's economic recovery after the catastrophic events of the previous year. This

reflects the willingness of businesses to innovate and expand rapidly after the severe challenges of the past. The main factors behind the resumption of investment activity in the economy were the need to finance capital investments in the defense industry and to rebuild the destroyed infrastructure.

These initiatives were implemented primarily with public funding, although significant support was also provided by international partners, in particular for the restoration of social infrastructure and transport infrastructure. In 2023, the gross domestic product in Ukraine's economy increased by more than USD 5 milliards, which is almost 18 times more than in 2022. Most of the increase in gross domestic product was achieved through reinvestment of income earned by foreign investors, which amounted to almost USD 3 milliards. However, due to still relatively high risks, foreign investors are cautious about entering the Ukrainian market. In 2023, the increase in gross domestic product in the form of equity instruments exceeded the figure for 2022 by only USD 190 million. At the same time, foreign investors resumed their investments in the Ukrainian economy through debt instruments, which amounted to USD 525 million in 2023.

Since the beginning of the large-scale war, the labor force in Ukraine has decreased by almost 6 million people of working age (including 1 million people mobilized for defense, almost 5 million people left Ukraine), while the share of people planning to return home from abroad is decreasing. At the same time, the number of unemployed in Ukraine decreased in December 2023, as reported by the State Employment Service. The data shows that 483 thousand unemployed people were registered, which is 46% less than in the previous year. This reduction in unemployment can be explained by the creation of employment opportunities within the economy, excluding external migration and the impact of mobilization processes. The improvement in employment rates indicates a positive trend in the labor market and economic stabilization in Ukraine after the consequences of a full-scale invasion in 2022. Moreover, inflation in Ukraine peaked at almost 26% year-on-year in December 2022 and has been steadily declining due to various factors, such as currency stability, sufficient domestic food supply, lower global commodity prices and rapid business adaptation to new challenges related to the war. As of February 2024, consumer inflation decreased by 4% year-on-year.

Table 1 - Detailing of economic security risks

<i>macro-economic security</i>	capital outflow from the economic territory of Ukraine and relocation of businesses abroad; significant reduction in investment activity; critical decline in credit financing of fixed assets, working capital and investments; reduction of labor potential due to intensive processes of migration abroad, a significant share of internally displaced persons, civilian casualties due to hostilities; growth of the consumer price index (inflation)
<i>financial security</i>	deterioration of the financial sustainability of the pension system; high state budget deficit; significant loss of tax and customs revenues; lack of trust of the public and business in the authorities; underfunding of certain budget expenditure items; growth of public debt; deterioration of the institutional capacity of the banking system
<i>industrial</i>	increased dependence of the domestic market on imports; reduction of

<i>security</i>	industrial production; acceleration of deindustrialization of the national economy; decreased competitive position of domestic producers in the domestic and foreign markets; increased share of low-quality technological and raw material products
<i>investment and innovation security</i>	reduction of public capital investments; curtailment of innovation activity in the national economy; deterioration of the dynamics of investment processes; insufficient funding for research and development; reduction of capital investments in various sectors
<i>externally economic security</i>	significant loss of export potential due to destruction or damage to production facilities; complications in transportation logistics; limitations in the effectiveness of the infrastructure supporting foreign trade; increase in the share of imports in domestic consumption
<i>food security</i>	food shortages; reduced production of agricultural products; destruction of the infrastructure for the production, processing and storage of agricultural products; shortage of labor resources in agricultural production
<i>social security</i>	deterioration of the socio-economic situation of vulnerable groups of the population; reduced capacity of the social protection system; deepening of structural imbalances in the labor market; decline in the welfare and quality of life of the population; worsening of access to social services; significant deterioration of the environment

In 2022, industrial production declined by almost 37%. However, starting in February 2023, the industry managed to improve its performance somewhat, which contributed to the establishment of an upward trend in production - in 2023, industrial production increased by 6% compared to 2022.

Ukraine's dependence on imports of goods in 2023 is now high. Imports of goods to Ukraine increased by 15% in 2023 compared to 2022. The share of imports in domestic consumption of industrial products was 46% in 2023 compared to 43% in 2022. First of all, machine building is the most import-dependent industry with an 83% share of imports in domestic consumption in 2023. The chemicals industry also maintains a high level of import dependence at 71%, relying mainly on imports from China.

As of January 2024, total estimated losses of industrial assets amounted to approximately \$13 milliard, which is approximately 16% higher than the estimate in February 2023. The value of destroyed assets of the Ukrainian agricultural sector as a result of the full-scale invasion during this period increased by 19% in December 2023 compared to February 2023. The largest category of losses among agricultural assets is damaged and destroyed agricultural machinery, amounting to \$6 milliard, or 57% of all losses. This amounted to USD 6 billion, or 57% of all losses. Destruction of already produced products amounted to almost USD 2 milliard. USD, and livestock - 254 million USD.

The destructive processes in Ukraine's economy caused by the war have led to a significant deepening of imbalances in foreign trade. The negative balance of foreign trade in goods and services in 2022 increased almost 10 times, or to USD 26 milliard, compared to 2021. It is also worth noting that against the background of an outstripping decline in exports compared to imports, the negative balance in trade in goods increased by USD 8 milliard. In addition, domestic demand in Ukraine increased in 2023, which was

accompanied by a dynamic increase in imports of a significant part of goods. According to the State Statistics Service, total imports in 2023 increased by 15%, primarily due to an increase in demand for manufacturing products, which increased by 22%. This indicates positive dynamics in the economy and a possible expansion of the market for imported goods in Ukraine.

The general economic situation in Ukraine, problems with filling the state budget due to the full-scale war and the growing need to finance the defense sector have led to a significant reduction in funding for research and development. In 2022, spending on research and development in Ukraine decreased by almost 18%, and its share in gross domestic product decreased to 0.4% of gross domestic product. In 2023, the downward trend in funding continued, but at a slower pace, which can be explained by restrictions on cutting costs for scientific and research institutions without actually shutting them down. On the other hand, a certain level of funding for scientific research, primarily applied research, was maintained to develop new technological solutions for defense purposes and to strengthen the country's military potential.

Capital expenditures increased 3-fold in nominal terms in 2023 compared to 2022. Public spending on the development, procurement, modernization and repair of weapons, equipment and military hardware increased 4-fold in nominal terms.

With the outbreak of a full-scale war, the number of socially vulnerable categories of the population has increased significantly, with the total number of low-income families increasing by 48 thousand people; children with disabilities by almost 45 thousand people compared to pre-war levels; and the number of people with disabilities and special needs is also increasing. In addition, the unemployment rate remains high: in January 2024, it was 17%, and the State Employment Service currently reports 96 thousand unemployed people.

The problems of labor utilization are exacerbated by the deepening imbalances in the labor market. Moreover, the share of households with paid work as their main source of income has decreased to 53%, while the share of household's dependent on government transfers and humanitarian aid has increased to 60%.

In 2022, short-term surges in consumer demand may lead to the depletion of local stocks of certain products. However, the market is able to quickly rebalance by increasing production, importing or selling additional stocks. Awareness-raising initiatives and actions to ensure sustainable access to food for internally displaced persons who still face food insecurity are also important. In addition, in 2023, the production of significant agricultural products, especially livestock, declined. As of January 2024, the total number of cattle in all categories of Ukrainian farms amounted to 2,234 thousand heads, which is 3% less than in January 2023.

The full-scale war has a negative impact on agricultural workers and farmers. More than 150,000 farmers working in the food system have been directly affected by the war and forced to migrate. In addition, small-scale producers engaged in growing seasonal products, who played an important role in providing employment and income to the rural population, found themselves in a difficult situation (*Pigul N.G., Pigul E.I., 2024*).

Ukraine's economic security faces many challenges, such as inflation, corruption, currency instability, and others. However, it is important to remember that the government, the business community and citizens can work together to ensure the stability and development of the country's economy.

Ukraine's economic security remains one of the most important issues for the country. Despite internal and external challenges, such as aggression from Russia, the Ukrainian government is constantly working to improve the situation. In particular, it is important to strengthen the investment climate, make the economy more competitive and develop trade relations with other countries (*Pigul N.G., Pigul E.I., 2024*).

Ensuring a high level of economic security helps to reduce the risks of financial crises and ensure the stable development of the country's economy. Various measures, such as infrastructure development, business support, investment promotion, and financial sector reforms, can contribute to strengthening Ukraine's economic security.

It is important to minimize the risk of economic instability in Ukraine by implementing sound economic policies, facilitating investment and trade, and ensuring political stability. A diversified and resilient economy is key to securing the country's economic future.

Scientific and applied principles of ensuring economic security of Ukraine.

Challenges facing modern Ukraine, and recognizes that issues such as corruption, lack of state support for small and medium-sized businesses, instability of the financial system, and loss of control over key sectors of the economy pose a threat to its economic security. These challenges remain relevant despite the country's growth and development. It is crucial for Ukraine to address these issues to ensure long-term economic stability and prosperity (*Bondaruk T., Chekhovska M., Bondaruk O., 2024*).

The issue of ensuring economic security in Ukraine has become particularly urgent due to the ongoing military aggression and the imposition of martial law. The war creates new threats to the economic stability of the country, including physical destruction of infrastructure, shortage of skilled labor, risks to food security, and challenges to the functioning of the national economy in the context of ongoing hostilities. In these circumstances, it is increasingly important to support and find ways to adapt to new challenges to protect Ukraine's economic interests.

The importance of legal support in ensuring economic security is undeniable. The absence of an effective legal framework and system for regulating economic processes leads to embezzlement of public funds, non-compliance with tax laws, and violation of entrepreneurs' rights. This makes it difficult to create favorable conditions for investment and business development, which ultimately threatens the country's sustainable economic growth (*Bondaruk T., Chekhovska M., Bondaruk O., 2024*).

Ukraine has begun making efforts to strengthen its economic security. For example, on August 11, 2021, President Volodymyr Zelenskyy issued a decree on the decision of the National Security and Defense Council of Ukraine on the «Economic Security Strategy of Ukraine until 2025». This strategic document outlines key aspects of economic security, including assessing the state of economic security, countering challenges and threats to each component of the system, and outlines the main development strategies in the field of economic security.

Economic security includes various aspects, such as protection against external threats, stability of the financial system, effective risk and investment management, price and exchange rate stability, consumer protection and competition in the market. To ensure economic security, various means and methods are used, such as the development of legislation, the creation of effective control and supervision mechanisms, professional

development, and the development of innovations and technologies (Figure 4).

The importance of legal support for Ukraine's economic security, as well as the challenges and threats posed by corruption, imperfect legislation, lack of effective law enforcement mechanisms, and insufficient efforts to combat it.

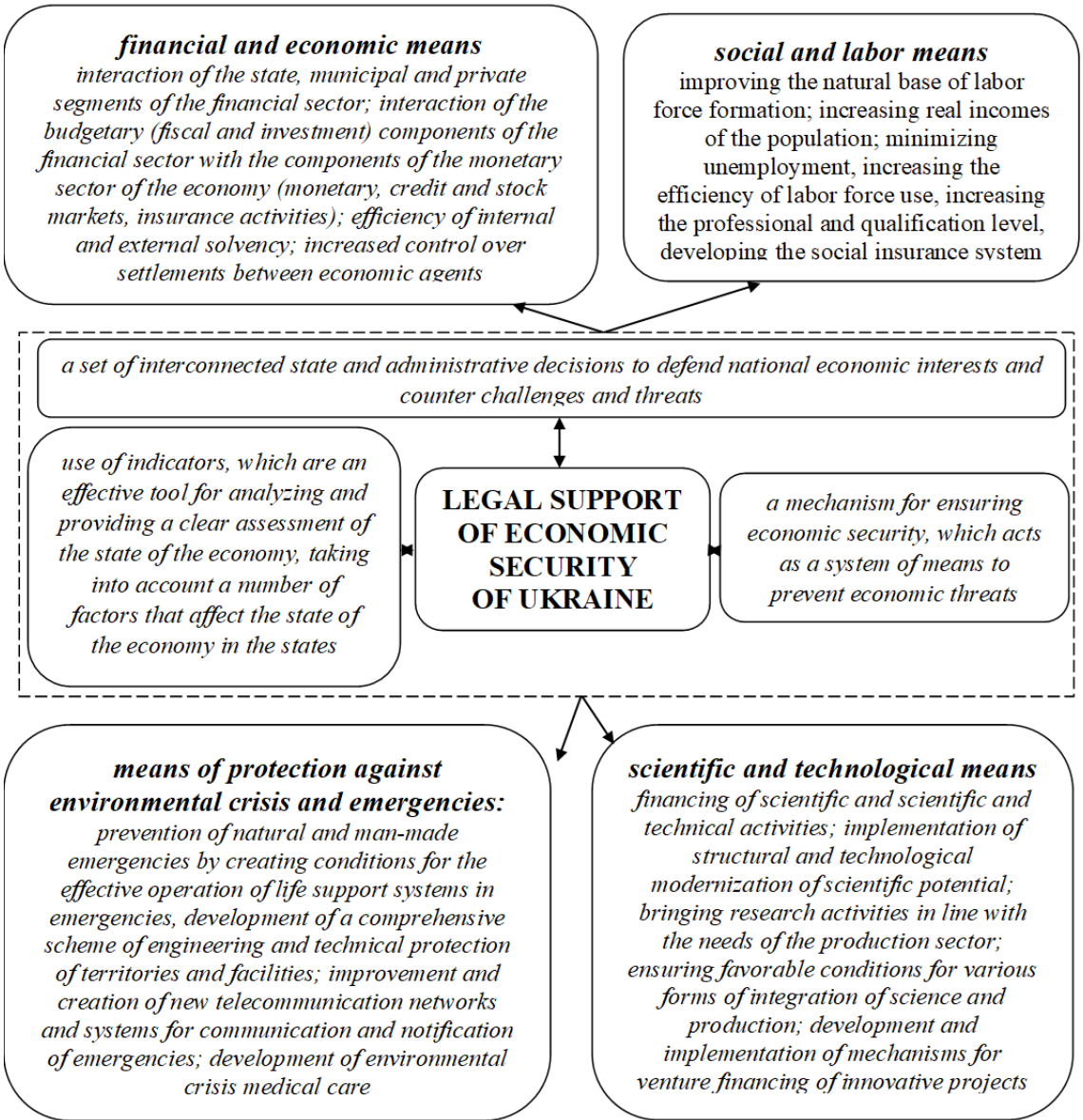


Figure 4. Main components of legal support for economic security of Ukraine

Source: developed by the author on the basis of (Lutsyk Y., 2023)

These problems do indeed impede the creation of a favorable environment for business development and investment. An effective legal framework and law enforcement are crucial for creating a stable and prosperous economy in any country.

To ensure economic security in Ukraine, systemic reforms in the legal sector are needed. It is important to create an effective legal framework that meets the current

challenges and requirements of the global market. The development and implementation of transparent and progressive rules, as well as strict enforcement measures, are critical elements of this process. For example, in the fight against corruption, it is really important to ensure the effectiveness of law enforcement agencies and the judiciary. The independence and integrity of the judiciary, control over the actions of public officials, and the implementation of transparent anti-corruption procedures are key steps to ensure economic security in the country (*Lutsyk Y., 2023*).

A comprehensive approach is indeed important in ensuring Ukraine's economic security. Active cooperation between the government, civil society, the business sector, and international partners is critical to achieving success in this endeavor. However, it is also important to take into account legal, institutional and political aspects when developing strategies to ensure the country's economic stability.

Ensuring Ukraine's sustainable economic security requires effective legal measures, which can only be implemented through decisive action and joint efforts of all stakeholders. The development of the rule of law, the fight against corruption, and the creation of favorable conditions for economic growth are key aspects to consider. It is important to establish control mechanisms and implement legal norms that will help maintain the stability and development of the country (*Moroz Yu., 2024*).

The use of information support is key to ensuring economic security. The speed and adequacy of the management decision-making process depends on the quality of information. Improvement of economic security performance indicators is also related to access to reliable and up-to-date data. Therefore, it is important to have access to information resources that can support the economic security management process.

Information support of economic security can be defined as the unity of accounting, analysis and audit systems united by information flows to manage economic processes, so it is justified to include an information support subsystem in the accounting and analytical support system, which ensures the integrated use of information resources by various functional subsystems (accounting, analysis, control, monitoring) (Fig. 5).

In the context of dynamic changes in the current economic situation, an important prerequisite is the formation of an effective economic security information system that will minimize internal and external threats and dangers, quickly navigate an unpredictable situation, and consistently achieve the set goals even in the face of uncertainty.

The modern world is constantly changing, and economic security is becoming increasingly linked to socioeconomic aspects. Ensuring the sustainability of the economy now also includes the principles of social justice, harmonious development, and meeting the social needs of the population (Figure 6).

The socio-economic support of Ukraine's economic security includes such aspects as the development of the social sphere, ensuring economic stability, improving living standards, entrepreneurship and investment activity. To ensure the economic security of the state, it is necessary to create a business environment that will facilitate the efficient functioning of the economy, as well as to implement social programs aimed at supporting vulnerable groups of the population. It is also important to ensure the stability of the country's financial and economic system and develop market relations.

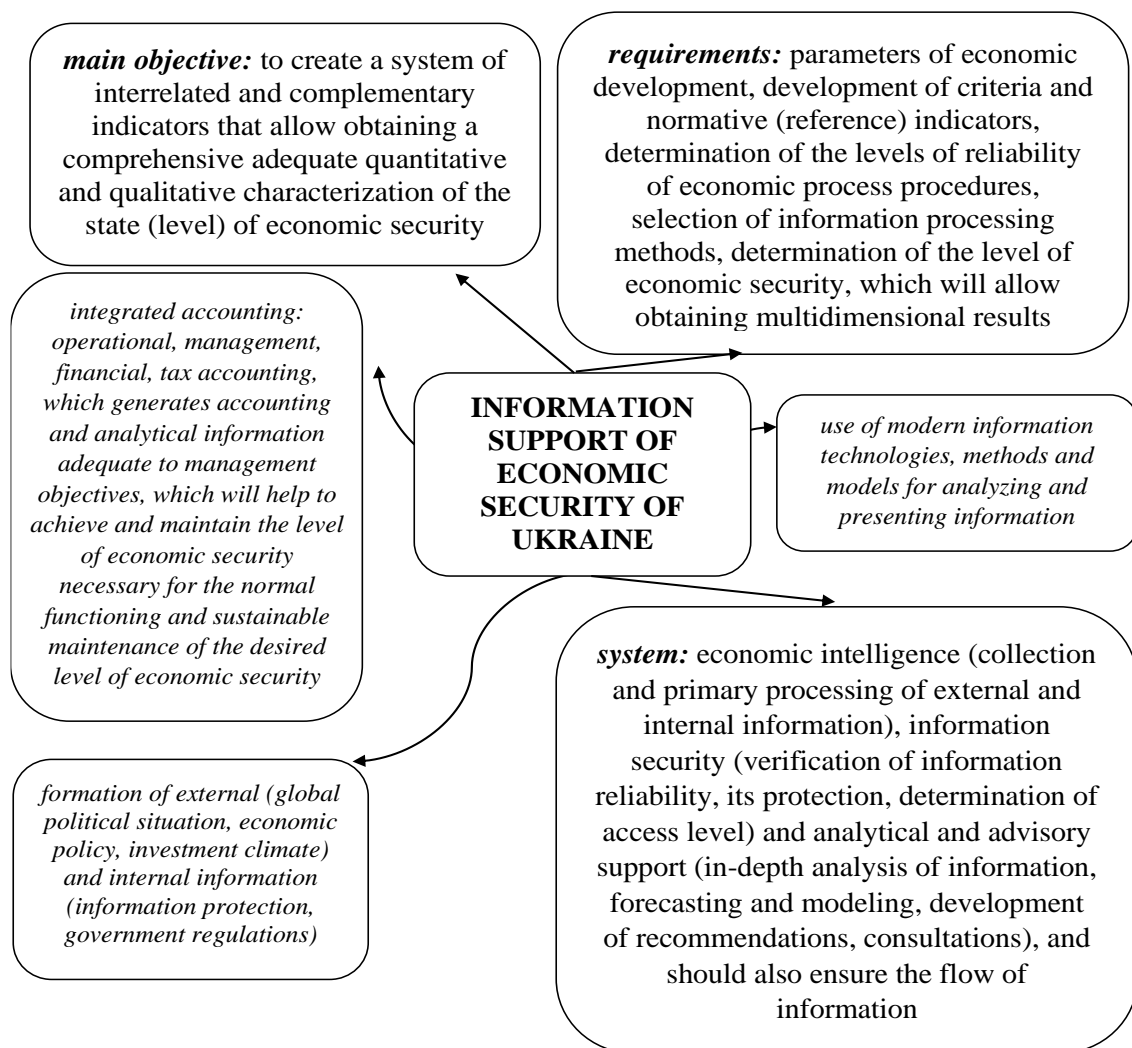


Figure 5. Main components of information support of economic security of Ukraine

Source: developed by the author on the basis of (Machak T., Dubyna O., Yurchenko S., 2024)

The direct implementation of actions to ensure economic security is carried out using a wide range of modern scientific and empirical methods aimed at increasing the competitiveness of the state's economic security systems (Figure 7).

Institutional and legal methods do play an important role in ensuring economic security and its development. The adoption of relevant state regulations helps to create a legal framework for the functioning of the national economy. In addition, these acts define the rules of the game in the market and ensure control over compliance with the law. Thus, institutional and legal methods are an important tool in ensuring the stability and development of the country's economy (Denysov O., 2018).

Organizational and administrative methods used to directly organize the work of national industries to ensure economic security can be effectively used both at the level of individual enterprises and at the level of the state. These methods include a number of

measures and strategies aimed at ensuring the sustainability and reliability of economic activity. Organizational methods may include the development and implementation of policies and procedures that promote effective economic security management, risk control, and timely prevention. At the state level, it is important to develop and implement comprehensive economic security strategies and programs aimed at supporting domestic producers and maintaining the sustainability of the country's economic system as a whole.

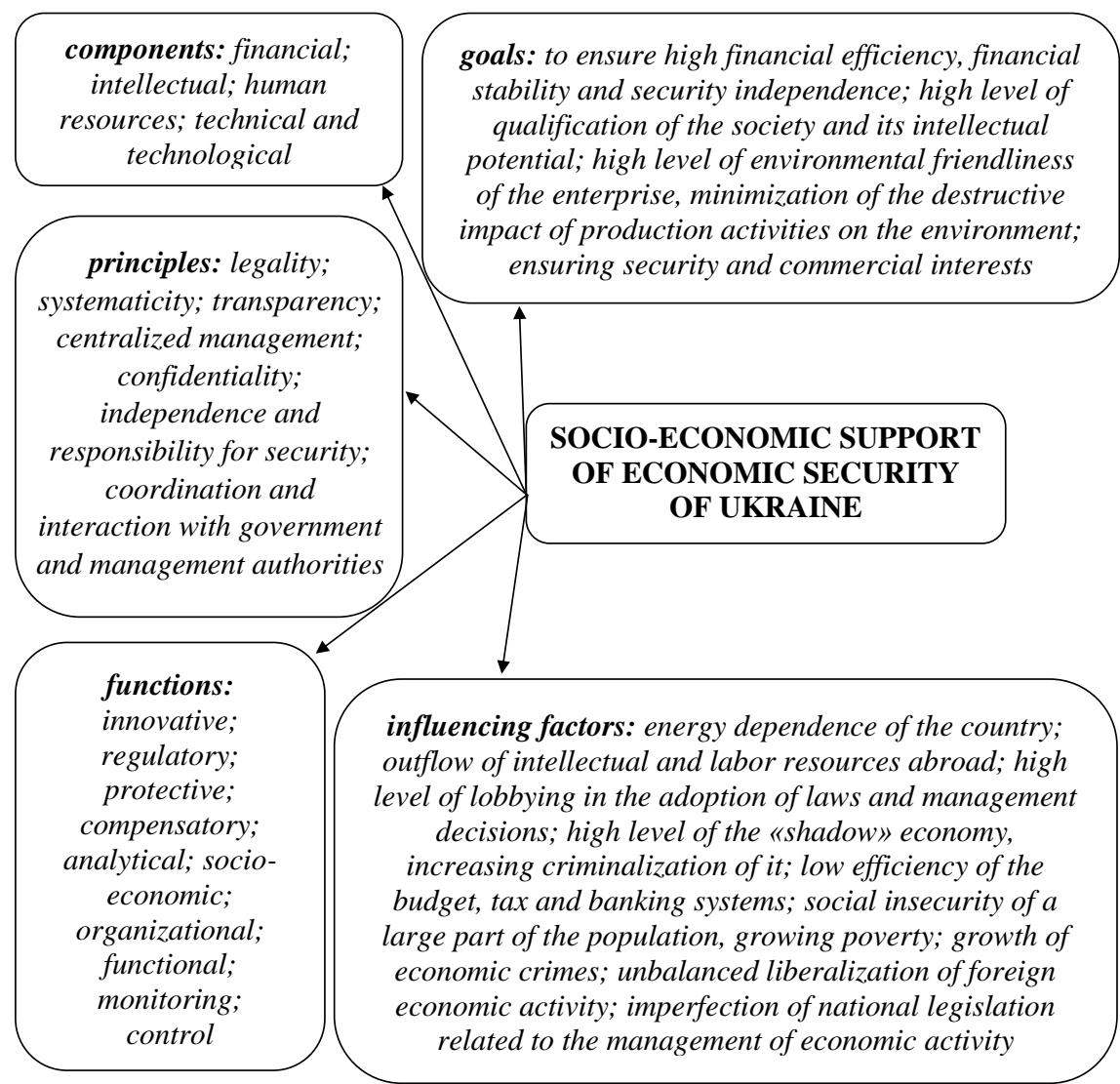


Figure 6. The main components of socio-economic support for Ukraine's economic security
 Source: developed by the author on the basis of (Ulyanova L.P., Chaika Y.M., Shchetinin A.I., 2023)



Figure 7. Modern methods of ensuring economic security of the state

Source: developed by the author on the basis of (Denysov O., 2018)

Socio-economic methods in ensuring economic security of industries, which are implemented through changes in the state tax, customs, depreciation policy, economic methods of state regulation in this matter, which are methods of both direct and indirect influence, by creating conditions for the effective functioning of enterprises, their innovative renewal, research and development activities, respectively, and increasing the competitiveness of the domestic economy. Effective economic methods include optimization of sources of investment in the development of industries, cost budgeting, lending to enterprises with the provision of state guarantees or the introduction of preferential lending for innovative development, renewal of enterprises in the industries, respectively, increasing their competitiveness, efficiency and security.

Effective methods include the adoption and implementation of state targeted industry development programs and regional development programs. In addition, the above methods provide social and psychological impact aimed at the population and the social sphere to form a positive attitude towards domestic products, increase the status and social level of domestic production, awaken psychological motives to increase consumption of domestic products and provide them with advantages over foreign ones,

respectively, form a model of consumer preferences for domestic goods and domestic industrial enterprises. At the state level, these methods are implemented by means of the state socio-economic policy aimed at improving the economic living standards of the population, the policy of supporting personal and personnel development, the level of education, health care, social protection, cultural development, etc.

Management and marketing methods involve the use of new innovative management methods in the development of domestic industries, such as performance management; quality management; process management methodology; implementation of international quality standards; implementation of organizational, modernization, restructuring, and reengineering of business processes. The use of development management methods makes it possible to increase the level of competitiveness and quality of the industry's products, accumulate resources, optimize resources and develop technical and technological processes, and build a system to ensure economic security.

The above methods help ensure an effective level of economic security of the state, as they allow to effectively monitor and analyze economic processes, identify potential threats and risks, and make informed decisions to ensure economic stability and protect national interests (*Denysov O., 2018*).

The effectiveness of economic security depends on various factors, including both methods and tools. The use of various tools and methods is one of the key aspects of successful economic stability and security. Indeed, the proper definition of differentiated tools for ensuring the economic security of the state is critical (Figure 8). This means taking into account various aspects of economic security, such as financial sustainability, technological development, raw material production, and other elements that may affect the economy. An effective strategy in this area will help ensure the sustainability of the country's economic development and protect it from external threats.

Through the use of effective tools to ensure economic security, the following algorithm of actions should be considered, which will allow to gradually, step by step to guide the state to achieve the desired sustainable state:

Stage 1 - collection and processing of information on the internal state and external environment of economic security, determination of the general economic situation in the country with forecasting the future vector of economic security development;

Stage 2 - identifying and assessing the level of risks, threats and hazards that are likely to arise in economic security;

Stage 3 - development of effective management decisions to implement a number of measures to overcome or minimize risks, threats and hazards in the event of their physical occurrence;

Stage 4 - development of effective algorithms of actions (measures) to counteract the impact of negative factors on economic security;

Stage 5 - monitoring and control by applying the proposed models and algorithms in practice;

Stage 6 - evaluating the effectiveness of the proposed methods and algorithms for overcoming risks, threats and hazards;

Stage 7 - continuous improvement of the economic security system.

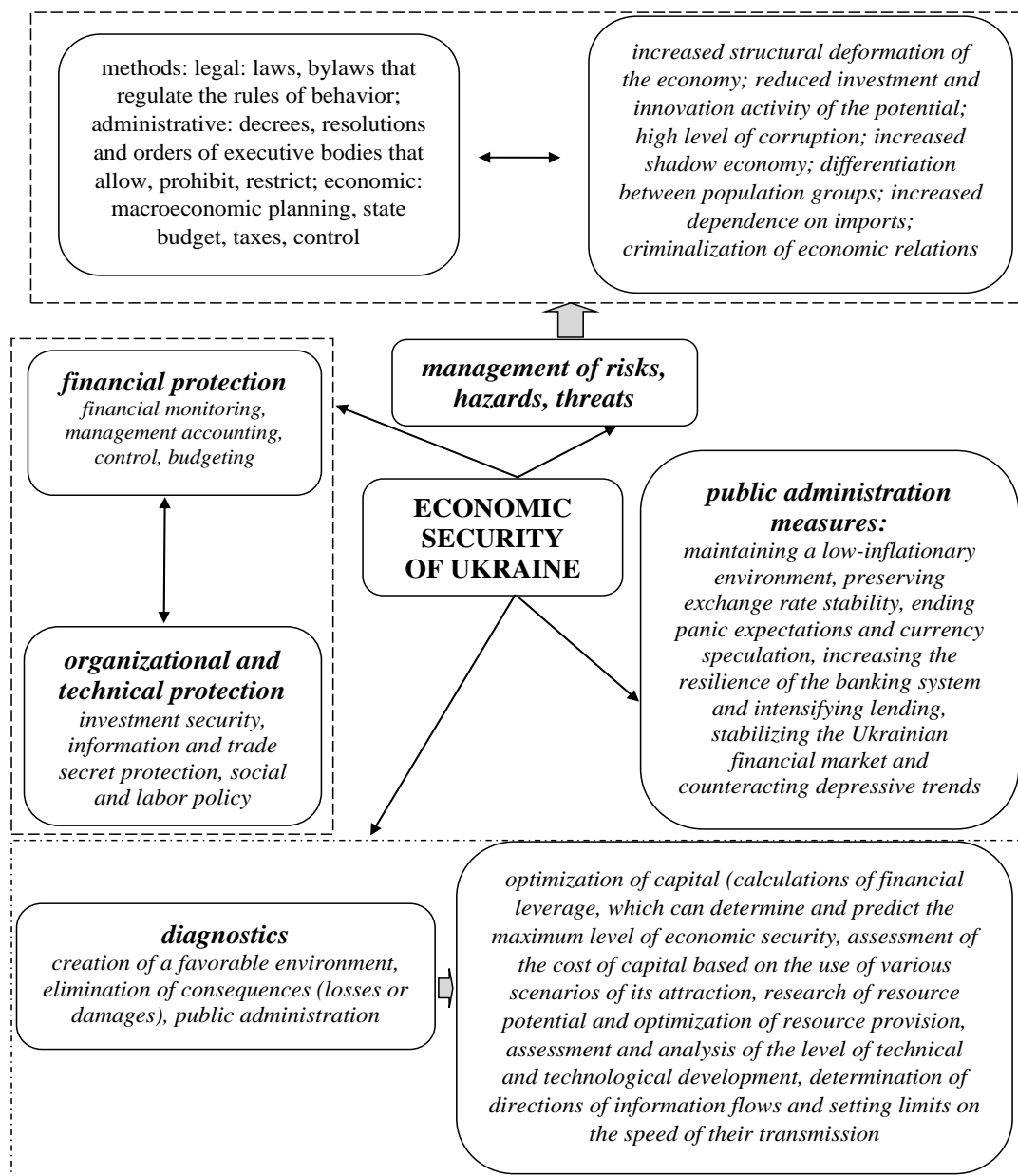


Figure 8. Tools for ensuring economic security of the state

Source: developed by the author on the basis of (Kopytko M., Zaverukha D., 2021)

Economic security is indeed critical to a country's stability. Ensuring it requires the continuous implementation of strategies and tactics, as well as operational actions. Some of the key steps that can help improve economic security include: first, risk analysis - thoroughly examining potential economic threats and risks that could affect the stability of the country; second, strategy development - developing strategies to protect and maintain economic security; third, implementation of controls - implementing necessary corrective actions to prevent potential threats; fourth, cooperation with partners - working with other

countries and international organizations to support the country's economic security. These steps can help ensure effective economic security and ensure the sustainability of the country's economy (*Kopytko M., Zaverukha D., 2021*).

Developing and implementing an effective economic security system is crucial in times of internal and external conflicts. A reliable economic security system is a guarantee of protection of national economic interests and the economic system as a whole from real and potential threats. The formation and development of the economic security system is a complex process that has its own logic and stages of implementation, functions in accordance with current needs and takes into account existing economic opportunities and requirements. In addition, ensuring the economic security of the state requires a systematic approach to tracking all possible threats to economic security and promptly responding to their manifestations through a comprehensive and perfect mechanism for ensuring the economic security of the state.

The conceptual goal of the process of ensuring economic security is to achieve a state of the national economy that creates favorable conditions for the development of an individual and strengthening the economic power of the state as a whole. An important prerequisite for the effective functioning of the economic security system is the definition of strategic priorities and the observance of national interests in all spheres of the national economy.

The purpose of creating an economic security system is to establish comprehensive guidelines for defending the interests of society in all sectors of the national economy and to create conditions for the accumulation and use of intellectual potential to ensure a higher level of economic security of the state.

The main tasks of the economic security system, in our opinion, are The main tasks of the economic security system are: protection of national interests and legal rights of all state subjects, including constitutional rights; collection, analysis, evaluation of data and forecasting of developments in the internal and external environment to identify threats; timely identification, analysis and assessment of real threats to economic security; decision-making and taking measures to counter threats and restore the economic security system to balance; prevention of crises and insecurity in the economy. These tasks help to ensure the stability of the economic environment, protect the interests of the state and citizens, and prevent crises and insecurity in the economy.

The development of mechanisms to ensure the economic security of the state is very important for sustainable development (Figure 9). Some of the above-mentioned means that can be used for this purpose include control over financial activities, detection and prevention of fraud and corruption, and development of risk management strategies.

The mechanism for ensuring economic security includes a number of instruments and strategies aimed at ensuring stability and development of various sectors of the economy. This may include legislation regulating economic activity, monitoring and analysis of economic processes, as well as measures to protect against external threats.

In the context of the author's research, the mechanism of ensuring economic security should be aimed at protecting, developing and reproducing intellectual potential as a strategic resource for the state. This may include measures to support education, science and innovation, as well as intellectual property protection and technology development. It is important to ensure interaction between various economic actors and government agencies to achieve optimal results in ensuring economic security.

The key prerequisites for the functioning of such a mechanism are the following: substantiation of the strategy and tactics of ensuring economic security; identification of the most important indicators of economic security, including intellectual security; monitoring of factors that pose a threat to the economic security of the state; economic diagnostics; analysis of the effectiveness of measures to ensure the economic security of the state. These prerequisites are necessary to create a reliable mechanism for protecting economic security and ensuring the prosperity of the nation.

The mechanism for ensuring the economic security of the state should meet the interests and priorities of society and the state and be aimed at achieving the set goals. It provides for a clear justification of goals and objectives, development of a long-term state policy to identify, prevent and eliminate threats to the economic security of the state. In addition, it should include a set of preventive measures implemented by all security actors and a system of immediate response measures in case of direct realization of the threat.

This mechanism is implemented through the use of specific economic, legal, administrative and other measures by state institutions. The mechanism for ensuring economic security involves the application of certain procedures and the implementation of specific actions aimed at guaranteeing the economic security of the state in the short term. In general, the developed and adopted mechanisms for ensuring economic security must meet clearly defined goals and outlined objectives of the economic security system.

Ensuring economic security has some key features, including the possibility of expanding the arsenal of instruments used in accordance with the defined goals and objectives. It is also important that the mechanism for ensuring economic security is adaptive, flexible, and can adequately respond to changes that have occurred as a result of adjustments to strategic guidelines, national priorities, and macroeconomic policy. The mechanism of ensuring economic security aims to create conditions for the accumulation and use of various potentials in order to guarantee a higher level of economic security of the state. This means developing strategies, policies, and instruments aimed at ensuring economic sustainability and protection against external threats.

An important component of the economic security mechanism is the various levers that can be used to influence the security object. These can be both direct measures (e.g., implementation of legislation or strategies) and indirect measures (e.g., stimulation of a certain sector of the economy or regulation of markets). Proper use of these levers helps to ensure the stability and resilience of the country's economy.

Leverages play an important role in ensuring effective control and management of important aspects of social life, including economic security. They are a tool for influencing and regulating risks that may arise in various areas of activity. For example, in finance, leverage is used to ensure the stability of the financial system and prevent crises. In the security sector, leverage can be used to strengthen measures to counter terrorism or cyberattacks. In this way, levers help to balance and strengthen the system of protection and counteraction in national industries. Legal levers are used to regulate legal norms and establish goals, main tasks and directions of the state's activities in the intellectual sphere. Economic levers are used to regulate processes in the economic sphere, monitor potential threats and neutralize real ones. Financial levers allow the state to ensure financial regulation and create monetary funds for potential compensation of losses caused by the realization of threats (*Levkina R.V., Kotko Ya.M., Kulinich O.A., 2024*).

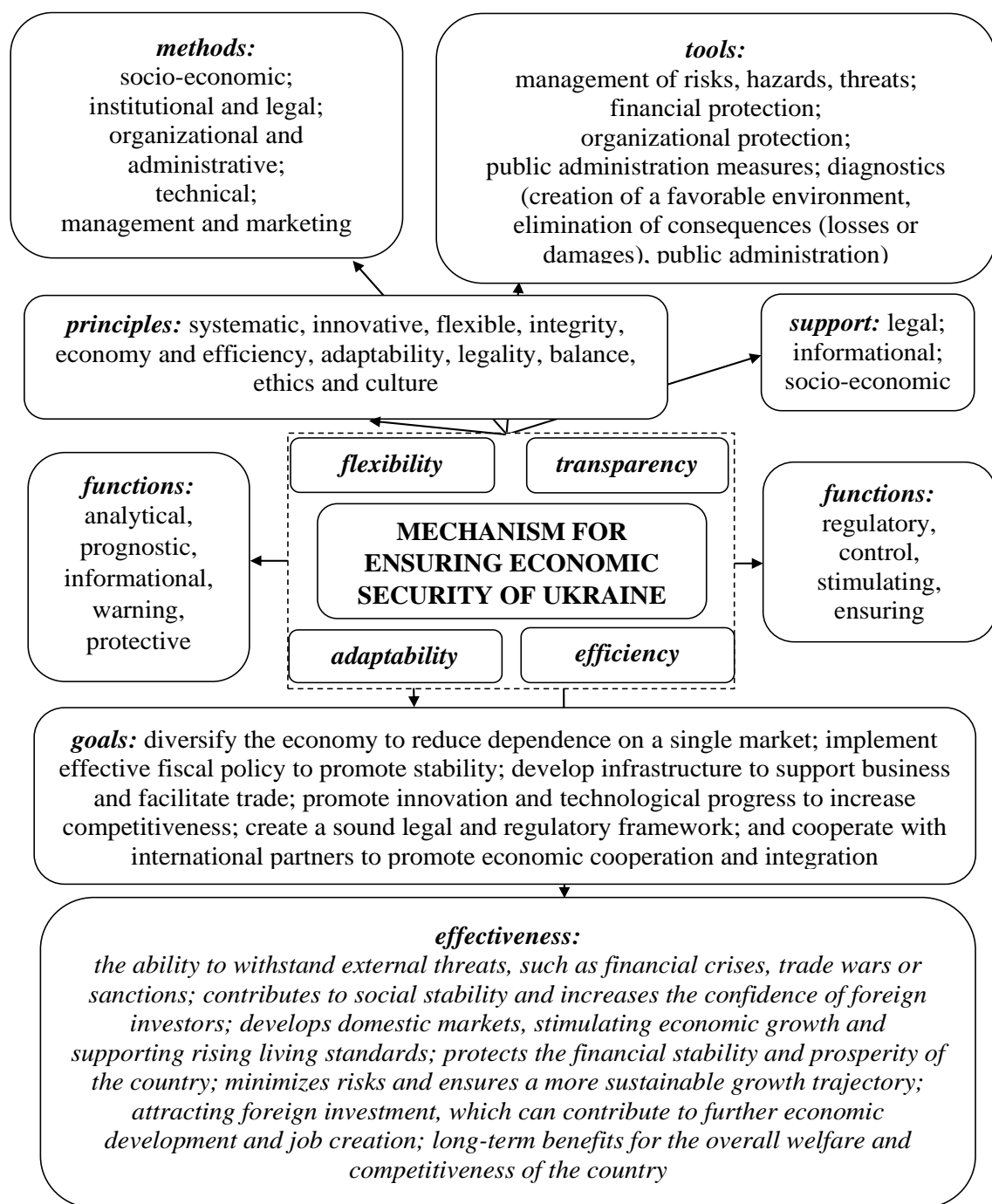


Figure 9. Mechanism of ensuring economic security of Ukraine

Source: developed by the author on the basis of (Levkina R.V., Kotko Ya.M., Kulinich O.A., 2024)

The mechanism of ensuring the economic security of the state is characterized by a comprehensive and effective coordinated toolkit used to increase the level of economic security and guarantee favorable conditions for economic and social development, increase

the competitiveness of the national economy, and increase the welfare of citizens. The use of the economic security mechanism implies the state's desire to achieve its fullest possible compliance with the requirements of macroeconomic policy in a particular period, which makes it possible to fully realize its goals and objectives.

The mechanism of ensuring the economic security of the state has a number of advantages, first of all:

1. Development and implementation of strategic economic programs that contribute to the stability and prosperity of the country;
2. Implementation of an effective system of monitoring and control over economic processes to prevent potential threats;
3. Promoting the development of competitive business and innovative projects to strengthen the economy;
4. Creating a climate favorable for investment and business development that increases the confidence of foreign and domestic investors;
5. Ensuring the stability of the financial system and minimizing risks to the economy.

The economic security system is an important structural component of national security, as it is determined by interdependent and interrelated components, such as functional, structural and spatial-territorial, which interact with each other and with the external environment for the effective functioning of the system as a whole. The stable functioning of the main subsystems of economic security ensures the sustainability and strength of the real and financial sectors of the economy, promotes long-term economic growth and improves the quality of life of the population.

The above studies show that both internal and external threats have intensified, significantly reducing the level of economic security. Awareness of the significance of all real and potential threats is important because they determine the state's policy in developing measures to prevent them, serving as a guide for all business entities in the formation and implementation of development strategies.

The mechanism of ensuring the economic security of the country shapes development strategies, in particular by assessing and overcoming risks, implementing policies aimed at ensuring stability and growth, increasing competitiveness, promoting innovation and sustainable development. This implies a proactive approach to managing economic challenges and seizing opportunities to support the overall well-being and sustainability of the country. Moreover, having a sustainable development strategy in place is crucial to ensuring the country's economic security in the long run. By focusing on sustainable practices and policies, a country can better manage its resources, reduce its environmental impact, and promote long-term economic growth. This approach not only benefits the current generation, but also ensures that future generations can thrive in a stable and secure environment (*Levkina R.V., Kotko Ya.M., Kulinich O.A., 2024*).

The state's sustainable development strategy provides an integrated approach to economic, environmental and social development that helps to meet the needs of the current generation without compromising the ability of future generations to meet their needs. This includes the rational use of resources, preservation of natural ecosystems, support for social justice, and implementation of economic mechanisms aimed at sustainable growth.

The state's sustainable development strategy and economic security are key concepts for ensuring sustainable economic growth and the nation's well-being. A sustainable

development strategy involves combining economic development with environmental protection and social responsibility. This means that economic achievements must be balanced with environmental protection and social justice. As for economic security, it is an important aspect for the efficiency and sustainability of the state's economy. Economic security is about ensuring the stability of the financial system, protecting the domestic market from external threats, developing competitiveness, and ensuring equal access to economic resources for all citizens. Attracting talented professionals from various fields, applying the latest technologies and implementing innovative solutions will help achieve these strategic goals to increase the sustainability of the country's development and maintain economic security (*Levkina R.V., Kotko Ya.M., Kulinich O.A., 2024*).

From these aspects, it can be concluded that effective economic security of the state requires a comprehensive approach that takes into account not only the tools but also the overall economic, political and social environment. It is important to choose and use tools taking into account the specific conditions prevailing in the country, which will help to increase the effectiveness of economic security measures. In this case, it is necessary to develop and use a mechanism to ensure the economic security of the state, as this can help ensure the stability and prosperity of the country in the face of economic challenges and threats. Economic security includes measures to maintain financial stability, develop infrastructure, promote innovation and support entrepreneurship. Ensuring economic security helps to preserve and strengthen the country's economic potential and ensure its compliance with global economic challenges (*Kovalenko V., 2024*).

The mechanism of ensuring economic security is a set of organizational and managerial measures aimed at preventing threats to the economic system. To ensure economic sustainability, it is important to develop strategies and policies aimed at strengthening the country's competitiveness and creating conditions for attracting investment and developing entrepreneurship. It is also important to constantly monitor economic and political risks and respond to them in a timely manner to avoid negative consequences for the national economy.

Thus, the economic security of the state is indeed a key element of the development of any country, including Ukraine. Ensuring the stability of the economy, protecting domestic resources and countering threats from external influences is critical to ensuring the prosperity of the nation and maintaining social stability. Actions to strengthen economic security, such as reforms, investment in infrastructure, and support for entrepreneurship, can contribute to growth and welfare (*Kovalenko V., 2024*).

The combination of economic security and sustainable development is an extremely important aspect of the modern world. Economic security helps to ensure the stability and prosperity of the country's economy, ensuring social and economic development. Sustainable development, on the other hand, involves the balanced use of resources and preservation of the environment for future generations. By combining these two aspects, a state can ensure long-term sustainability and prosperity for its population.

Sustainable development of the state is a very important strategy, as it helps to preserve natural resources, ensures social stability, improves living standards and promotes economic growth. This means that the country must develop economically, socially and environmentally in a way that balances current needs. Successful implementation of the sustainable development concept will create a sustainable foundation for future generations.

Sustainable development of the state is important not only for economic prosperity, but also for the security of the state. For a country to be stable and prosperous, it is important to ensure both economic development and protection from external threats. This means developing infrastructure, economic resilience, and strengthening the country's defense capabilities. It is also important to maintain sustainable social programs and political stability to ensure the comprehensive development of the state.

To achieve sustainable development, it is necessary to ensure an effective level of economic security of the state. This means developing an economy that promotes balanced growth, optimal use of resources, and reduction of negative environmental impacts. It is necessary to develop green development strategies, introduce environmentally friendly technologies, and continuously improve mechanisms for controlling the use of resources. This will help create a sustainable and environmentally friendly environment for current and future generations.

Conclusion. The economic security of the state plays an extremely important role in the sustainable development of the country. This is an important aspect because a stable economy helps to ensure the living standards of citizens, attract investments, create new jobs, and ensure the effective functioning of the entire public administration system. In addition, economic security also helps to reduce the risks of economic crises and helps the country to move forward confidently on the path to sustainable development. The main components of economic security are economic stability, effective financial management, food security, infrastructure development, business competitiveness, protection of intellectual property and customs space, reasonable use of resources and energy efficiency.

The general challenges to the economic security of the state include dependence on imports, insufficient competitiveness of production, high unemployment, tax and financial crises, and insufficient innovation of the economy. In addition, the economic security of the state may be threatened by various risks. For example, political instability, trade wars, financial crises, inflation, corruption and other factors may threaten the country's economic security. It is important to constantly monitor these risks and develop strategies to prevent them.

Ensuring the economic security of the state is an extremely important task to ensure the stability and prosperity of the country. Effective management of the economy, banking system and financial resources are key components of this process. It is important to develop strategies and policies aimed at protecting the economic interests of the state and guaranteeing financial stability.

The multi-vector provision of the state's economic security includes various aspects, such as legal, informational, and socio-economic. Legal support involves the creation of an effective system of laws and rules that regulate economic activity to prevent corruption and misconduct. Information support includes providing access to reliable and up-to-date information on the economic situation in the country and the world. Socio-economic support involves creating conditions for sustainable economic development and supporting social protection of citizens. Taking into account all these aspects, the state can achieve the sustainability of its economy and improve the living standards of its citizens.

Various methods are used to effectively ensure the economic security of the state. First of all, these include socio-economic, institutional and legal, organizational and administrative, technical, and management and marketing measures. These methods are

aimed at ensuring sustainable economic development and improving the living standards of citizens. Moreover, to ensure the economic security of the state, not only various methods are used, but also modern tools. These tools include monitoring of economic processes, risk analysis, development of development strategies, and the use of specialized programs and technologies to protect the economic interests of the state.

It is important to continuously improve this toolkit, as current challenges and threats to economic security are constantly changing.

The development and implementation of the economic security mechanism are important aspects for the stability of the country. Economic security is essential to ensure the development and prosperity of the state, so it is important to take measures to protect the economy from external threats, ensure the stability of the financial system and regulate economic processes. Implementing a mechanism to ensure Ukraine's economic security has a number of advantages, including reducing the risk of economic crises and maintaining the stability of the national economy; protecting domestic enterprises and state interests in the context of globalization; increasing the competitiveness of domestic enterprises in the international market; stimulating investment and development of the national economy; improving the living standards of the population and meeting their social needs. These are just a few of the benefits that may result from the implementation of such a mechanism.

The mechanism of ensuring economic security in Ukraine helps to ensure sustainable development of the state. Economic security involves protecting the country's economic resources, maintaining financial stability, and promoting economic growth to ensure the welfare of citizens. By implementing effective policies and strategies to protect against external and internal threats, Ukraine can create a favorable environment for economic growth and development.

Economic security indeed plays an important role in the country's sustainable development. Ensuring economic security is an extremely important task, as it contributes to the stability of the economy, provides protection against external threats, and helps to maintain the country's financial stability. The development of effective socio-economic and environmental policies is a key factor in ensuring the country's economic security.

References:

- Козловський С., Горун С., Мамашвілі Л. Підвищення економічної безпеки держави на основі інноваційних та цифрових трансформацій. *Економіка та суспільство*. 2024. 59. <https://doi.org/10.32782/2524-0072/2024-59-34>
- Маслій О., Ківшик О., Котелевець М. Загрози економічній безпеці держави в умовах глобальних перетворень. *Економічний простір*. 2023. 183. С. 25-30. <https://doi.org/10.32782/2224-6282/183-4>.
- Корнієнко Т. Аналіз стану економічної безпеки України та пріоритети її зміцнення. *Економіка та суспільство*. 2022. 38. <https://doi.org/10.32782/2524-0072/2022-38-61>
- Генералов О., Романенко О. Національна економічна безпека України в умовах глобальних викликів. *Молодий вчений*. 2021. 11 (99). С. 357-361. <https://doi.org/10.32839/2304-5809/2021-11-99-78>
- Пушак Я., Трушкіна Н. Правове забезпечення економічної безпеки держави в умовах індустрії 4.0. *Цифрова економіка та економічна безпека*. 2022. 1 (01). С.135-142. <https://doi.org/10.32782/dees.1-22>.
- Черевко І., Фляк Ю. Економічна безпека: сутність, значення і детермінанти. *Аграрна економіка*. 2024. Т. 17, № 1. С. 3-16. <https://doi.org/10.31734/agrarecon2024.01.003>.

- Молдован О.О. Сучасні методологічні виклики теорії економічної безпеки держави як самостійної наукової дисципліни. *Економіка та держава*. 2021. № 7. С. 10–15. DOI: [10.32702/2306-6806.2021.7.10](https://doi.org/10.32702/2306-6806.2021.7.10).
- Лизун М.В., Озарко К.С. Економічна безпека ЄС та України: нові виклики та загрози. *Вісник мариупольського державного університету серія: економіка*. 2023. Вип. 25. С. 117-127. DOI 10.34079/2226-2822-2023-13-25-117-127
- Дмитрова О.С., Терещук О.Д., Карпова К.В. Теоретичні аспекти формування системи економічної безпеки держави. *Публічне управління і адміністрування в Україні*. 2023. Випуск 37. С. 173-177. <https://doi.org/10.32782/pma2663-5240-2023.37.32>
- Пігуль Н.Г., Пігуль Є.І. Економічна безпека держави: сутність та актуальні загрози. *Бізнес-інформ*. 2024. № 7. С. 6-13. <https://doi.org/10.32983/2222-4459-2024-7-6-13>.
- Бондарук Т., Чеховська М., Бондарук О. Економічна безпека України під час військових дій: виклики та шляхи протидії. *Економічні горизонти*. 2024. 1(27). С. 129–141. [https://doi.org/10.31499/2616-5236.1\(27\).2024.299201](https://doi.org/10.31499/2616-5236.1(27).2024.299201)
- Луцик Ю. Економічна безпека в умовах глобальних викликів та загроз. *Таврійський науковий вісник. Серія: Економіка*. 2023. (15). С. 74-83. <https://doi.org/10.32782/2708-0366/2023.15.9>.
- Мороз Ю. Механізм забезпечення управління економічною безпекою в умовах динамічних і структурних змін розвитку національної економіки України. *Суспільство та безпека. Управління національною безпекою*. 2024. № 1 (2). С. 131-140. [https://doi.org/10.26642/sas-2024-1\(2\)-131-140](https://doi.org/10.26642/sas-2024-1(2)-131-140)
- Мачак Т., Дубина О., Юрченко С. Інформаційне забезпечення управління системою економічної безпеки підприємства та його удосконалення. *Економіка та суспільство*. 2024. (61). <https://doi.org/10.32782/2524-0072/2024-61-66>
- Ульянова Л.П., Чайка Ю.М., Щетинін А.І. Війна як чинник підвищення соціально-економічної небезпеки в Україні. *Держава та регіони. Серія: Економіка та підприємництво*. 2023 р. № 4 (130). С. 51-57. <https://doi.org/10.32782/1814-1161/2023-4-8>
- Денисов О.Є. Основні методи механізму забезпечення економічної безпеки галузі. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство*. 2018. Випуск 17, частина 1. С. 95-99.
- Копитко М., Заверуха Д. Характеристика основних складових забезпечення економічної безпеки держави. *Вчені записки Університету «КРОК»*. 2021. (3(63)). С. 155–160. <https://doi.org/10.31732/2663-2209-2021-63-155-160>
- Levkina R.V., Kotko Ya.M., Kulinich O.A. Mechanism of sustainable development of business entities in the system of international economic relations. *Економічний журнал Одеського політехнічного університету*. 2024. 4 (30). С. 57–67. DOI: <https://doi.org/10.15276/EJ.04.2024.7>.
- Коваленко В.В. Складові забезпечення економічної безпеки при сталому розвитку України. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*. 2024. Том 35 (74) № 5. С. 51-56. <https://doi.org/10.32782/TNU-2707-0581/2024.5/09>.

References:

- Kozlovskiy S., Horun S., Mamashvili L. Pidvyshchennia ekonomichnoi bezpeky derzhavy na osnovi innovatsiinykh ta tsyfrovyykh transformatsii. *Ekonomika ta suspilstvo*. 2024. 59. <https://doi.org/10.32782/2524-0072/2024-59-34>
- Maslii O., Kivshyk O., Kotelevets M. Zahrozy ekonomichnoi bezpetsi derzhavy v umovakh hlobalnykh peretvoren. *Ekonomichniy prostir*. 2023. 183. S. 25-30. <https://doi.org/10.32782/2224-6282/183-4>
- Korniienko T. Analiz stanu ekonomichnoi bezpeky Ukrainy ta priorityty yii zmitsnennia. *Ekonomika ta suspilstvo*. 2022. 38. <https://doi.org/10.32782/2524-0072/2022-38-61>.
- Heneralov O., Romanenko O. Natsionalna ekonomichna bezpeka Ukrainy v umovakh hlobalnykh vyklykiv. *Molodyi vchenyi*. 2021. 11 (99). S. 357-361. <https://doi.org/10.32839/2304-5809/2021-11-99-78>
- Pushak Ya., Trushkina N. Pravove zabezpechennia ekonomichnoi bezpeky derzhavy v umovakh industrii 4.0. *Tsyfrova ekonomika ta ekonomichna bezpeka*. 2022. 1 (01). S.135-142. <https://doi.org/10.32782/dees.1-22>.

- Cherevko I., Fliak Yu. Ekonomichna bezpeka: sutnist, znachennia i determinanty. *Ahrarna ekonomika*. 2024. T. 17, № 1. S. 3-16. <https://doi.org/10.31734/agrarecon2024.01.003>.
- Moldovan O.O. Suchasni metodolohichni vyklyky teorii ekonomichnoi bezpeky derzhavy yak samostiinoi naukovoï dystsypliny. *Ekonomika ta derzhava*. 2021. № 7. S. 10–15. DOI: 10.32702/2306-6806.2021.7.10.
- Lyzun M.V., Ozarko K.S. Ekonomichna bezpeka YeS ta Ukrainy: novi vyklyky ta zahrozy. *Visnyk mariupolskoho derzhavnoho universytetu seriia: ekonomika*. 2023. Vyp. 25. S. 117-127. DOI 10.34079/2226-2822-2023-13-25-117-127
- Dmytrova O.S., Tereshchuk O.D., Karpova K.V. Teoretychni aspekty formuvannia systemy ekonomichnoi bezpeky derzhavy. *Publichne upravlinnia i administruvannia v Ukraini*. 2023. Vypusk 37. S. 173-177. <https://doi.org/10.32782/pma2663-5240-2023.37.32>
- Pihul N.H., Pihul Ye.I. Ekonomichna bezpeka derzhavy: sutnist ta aktualni zahrozy. *Biznes-inform*. 2024. № 7. S. 6-13. <https://doi.org/10.32983/2222-4459-2024-7-6-13>
- Bondaruk T., Chekhovska M., Bondaruk O. Ekonomichna bezpeka Ukrainy pid chas viiskovykh dii: vyklyky ta shliakhy protydii. *Ekonomichni horyzonty*. 2024. 1(27). S. 129–141. [https://doi.org/10.31499/2616-5236.1\(27\).2024.299201](https://doi.org/10.31499/2616-5236.1(27).2024.299201)
- Lutsyk Yu. Ekonomichna bezpeka v umovakh hlobalnykh vyklykiv ta zahroz. *Tavriiskyi naukovyi visnyk. Serii: Ekonomika*. 2023. (15). S. 74-83. <https://doi.org/10.32782/2708-0366/2023.15.9>
- Moroz Yu. Mekhanizm zabezpechennia upravlinnia ekonomichnoiu bezpekoiu v umovakh dynamichnykh i strukturnykh zmin rozvytku natsionalnoi ekonomiky Ukrainy. *Suspilstvo ta bezpeka. Upravlinnia natsionalnoiu bezpekoiu*. 2024. № 1 (2). S. 131-140. [https://doi.org/10.26642/sas-2024-1\(2\)-131-140](https://doi.org/10.26642/sas-2024-1(2)-131-140)
- Machak T., Dubyna O., Yurchenko S. Informatsiine zabezpechennia upravlinnia systemoiu ekonomichnoi bezpeky pidpriemstva ta yoho udoskonalennia. *Ekonomika ta suspilstvo*. 2024. (61). <https://doi.org/10.32782/2524-0072/2024-61-66>
- Ulianova L.P., Chaika Yu.M., Shchetynin A.I. Viina yak chynnyk pidvyshchennia sotsialno-ekonomichnoi nebezpeky v Ukraini. *Derzhava ta rehiony. Serii: Ekonomika ta pidpriemnytstvo*. 2023 r. № 4 (130). S. 51-57. <https://doi.org/10.32782/1814-1161/2023-4-8>.
- Denysov O.Ie. Osnovni metody mekhanizmu zabezpechennia ekonomichnoi bezpeky haluzi. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Serii: Mizhnarodni ekonomichni vidnosyny ta svitove hospodarstvo*. 2018. Vypusk 17, chastyna 1. S. 95-99.
- Kopytko M., Zaverukha D. Kharakterystyka osnovnykh skladovykh zabezpechennia ekonomichnoi bezpeky derzhavy. *Vcheni zapysky Universytetu «KROK»*. 2021. (3(63)). S. 155–160. <https://doi.org/10.31732/2663-2209-2021-63-155-160>
- Levkina R.V., Kotko Ya.M., Kulnich O.A. Mechanism of sustainable development of business entities in the system of international economic relations. *Ekonomichni zhurnal Odeskoho politekhnichnoho universytetu*. 2024. 4 (30). S. 57–67. DOI: <https://doi.org/10.15276/EJ.04.2024.7>.
- Kovalenko V.V. Skladovi zabezpechennia ekonomichnoi bezpeky pry stalomu rozvytku Ukrainy. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Serii: yurydychni nauky*. 2024. Tom 35 (74) № 5. S. 51-56. <https://doi.org/10.32782/TNU-2707-0581/2024.5/09>

CHAPTER 14. THE ROLE OF COMPUTER VISUALIZATION IN THE FORMATION OF MEDIA LITERACY: HOW DIGITAL IMAGES INFLUENCE OUR PERCEPTION OF INFORMATION

Inna I. KOVTANIUK

Teacher at the Department of Informatics and Information and Communication
Technologies, Tychyna Uman State Pedagogical University
(2, Sadova str, Uman, 20300, Ukraine)

i.kryvoruchko@udpu.edu.ua

<https://orcid.org/0000-0002-9886-9315>

Abstract. The article discusses the role of computer visualization as a key tool for influencing the modern information space. Visual content has become an integral part of communication in the digital age, which necessitates a critical approach to its analysis and interpretation. The author explores how computer visualization contributes to the effective transfer of knowledge, as well as how it can be used to manipulate the minds of the audience.

Particular attention is paid to the phenomenon of deepfakes and the use of artificial intelligence to create realistic but completely falsified images and videos. Such technologies have a wide range of applications – from educational and scientific to potentially dangerous, in particular in political manipulation and the spread of disinformation. In this regard, the importance of developing media literacy, including the ability to analyze and verify visual information, is emphasized.

It also discusses the positive aspects of using computer visualization, in particular in education, journalism, science, and mass communications. Visual tools such as infographics, 3D-models, animations, and interactive graphs help to improve the understanding of complex concepts and contribute to the quality of information perception.

Given the rapid development of digital technologies and their impact on society, the author emphasizes the need to develop critical thinking and skills of conscious consumption of content.

Keywords: Computer visualization, visualization, digital signage, media literacy, visual content.

Introduction. In today's information society, where visual content has become the main means of transmitting information, computer visualization plays an important role in shaping the perception of reality and critical thinking. Thanks to the development of digital technologies, people interact with a huge number of images every day: from photos and videos to complex infographics, animated presentations, and 3D-visualizations. Visual information penetrates all spheres of life – from education and science to mass media, advertising, and social networks. That's why the ability to critically analyze digital images and understand their impact on the perception of information is one of the key skills of media literacy (*Petko, 2024*).

Media literacy is defined as a set of knowledge and skills that allow a person to consciously perceive, analyze, verify and interpret information coming from various media resources. In the digital era, this is especially true, as computer visualization can both

contribute to the effective transfer of knowledge and be used to manipulate public opinion. The use of images in the media affects the emotional state of the audience, creates certain narratives, and sometimes can even distort reality (*Medvedieva, 2020*).

One of the main challenges of the modern information space is the spread of fake news, disinformation and manipulative content. The advent of artificial intelligence technologies, generative algorithms, and deep neural networks has made it possible to create realistic but completely fictional images and videos (the so-called deepfake). Such technologies can be used both for positive purposes (e.g., to recreate historical events or training simulations) and for destructive influence on the public (e.g., political manipulation, fabrication of compromising material, creation of false stories).

At the same time, computer visualization is a powerful tool for developing critical thinking and media analysis. Visual tools such as infographics, 3D-models, interactive graphs, and animations help people better understand complex information, facilitate the educational process, and improve the quality of data perception (*Melnychuk, 2023*). Educational and scientific institutions are actively using computer visualization to create educational materials, and journalists are using it to explain complex social, economic, or environmental phenomena.

Thus, the study of the role of computer visualization in the formation of media literacy is important not only for understanding the modern information environment, but also for ensuring the resilience of society to information threats. It is important not only to recognize visual manipulations, but also to understand the principles of image creation, learn to critically analyze content, and develop the skills of conscious information consumption.

1. Definition and essence of computer visualization

The current stage of education development is characterized by the rapid introduction of information technology, which opens up new opportunities for optimizing the educational process, as well as for creating more efficient and accessible conditions for learning. One of the key tools actively used in educational practice is computer visualization, which provides an interactive presentation of material, allows for a better understanding of abstract concepts, and promotes a better understanding of complex topics. It helps to transform complex theoretical knowledge into visual, understandable images, which significantly increases learning efficiency, reduces cognitive load, and activates students' cognitive activity (*Tkachuk, Bondarenko, 2024*).

Computer visualization has a special role in disciplines such as computer science, where many concepts are abstract and difficult to understand without visual representation. This applies to such important topics as algorithms, data structures, programming, computer graphics, and others (Fig. 1). The use of computer visualizations allows not only to understand the principles of complex systems, but also to carry out their experimental visualization, which allows students to visually observe processes that are difficult to imagine without special tools.

Thanks to computer visualization, students are able to better navigate complex theoretical issues, as visual tools allow them to turn abstract concepts into concrete, understandable illustrations. They can observe the dynamics of changes in real time, track the execution of algorithms, or examine data structures that would be difficult to comprehend without visual tools. For example, when studying sorting or search algorithms,

computer visualization allows you to see each step of the algorithm, which makes it much easier to understand (Shtaiier, Nazarov, Kravets, 2023).

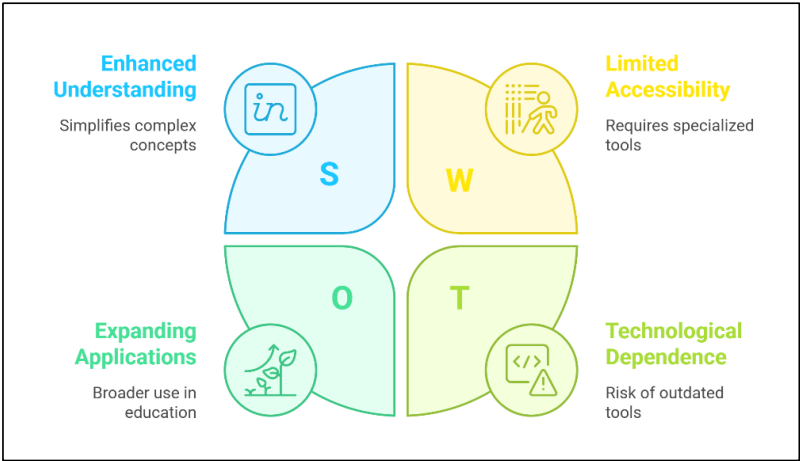


Fig. 1. Computer visualization in education

Computer visualization is also becoming a powerful tool for interactive learning. With the help of tools such as simulations, interactive graphs, or animations, students can not only observe processes but also actively interact with them by changing parameters or testing hypotheses (Fig. 2). This contributes to the development of critical thinking, in-depth understanding of the material, and the ability to apply the knowledge gained in practice. For example, a student can change the input data in an algorithm or vary the parameters of a data model, observing how this affects the result. This approach not only strengthens the understanding of theoretical aspects, but also allows you to develop skills in solving real-world problems.

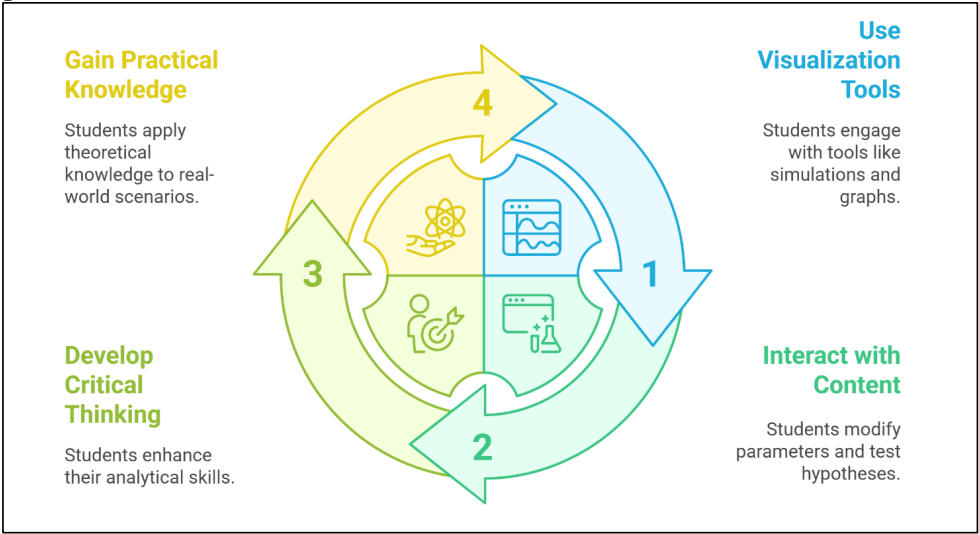


Fig. 2. Interactive learning cycle

Already at the early stages of learning with the use of computer visualization, one can see a significant reduction in the level of stress among students, as complex theoretical tasks cease to be abstract and difficult to understand. Visual tools provide access to information

in a form that is intuitive, allowing students to navigate new material faster. As a result, students become more engaged in learning, more motivated, and more interested in actively using technology in their educational process (Titova, 2024).

Computer visualization is a process that uses computer technology to create, process, and display graphical objects that help simplify the perception and understanding of information. It includes various forms of data representation, such as graphs, charts, 3D-models, and other visual elements.

This process starts with converting data into a graphical form. Using software allows you to create and manipulate these graphical objects. For example, statistical data can be transformed into graphs that demonstrate trends and correlations that may be less obvious in text form. To create such visualizations, a variety of algorithms are used to generate both static images and dynamic elements such as animations and interactive models.

One of the main functions of computer visualization is to simplify the perception of complex information. Instead of looking at large volumes of numbers or textual descriptions, users can understand data more quickly through visual elements such as graphs and charts. This is especially important for analyzing large data sets, where visualizations can quickly demonstrate key patterns and trends (Kryvoruchko, Allakulyiev, 2023).

Computer visualization also contributes to a better understanding of complex concepts. It allows you to represent abstract or complex ideas in an understandable way. For example, three-dimensional models can represent physical objects and their properties, which can be useful for learning in fields such as science, architecture, and engineering.

In the field of education, computer visualization is of great importance. It can improve the quality of the learning process by helping students to better absorb material through visual representations of complex topics (Fig. 3). Teachers can use visualizations to demonstrate theoretical concepts, conduct interactive lessons, and create dynamic learning environments that stimulate active learning and student engagement (Kryvoruchko, 2022).

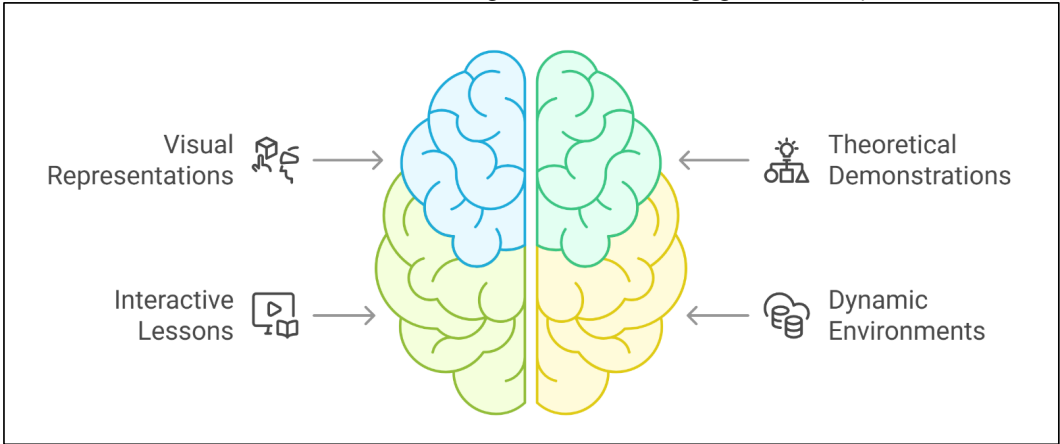


Fig. 3. Computer Visualization in Education

Computer visualization is also widely used in business and industry. For example, in marketing, visualizations are used to analyze consumer data, evaluate the effectiveness of advertising campaigns, and predict market trends. In manufacturing, three-dimensional models allow you to create product prototypes, optimize production processes, and conduct virtual tests before actual production begins.

In the medical field, computerized imaging provides revolutionary opportunities for diagnosis and treatment. Modern methods, such as visualization of internal organs using CT (computed tomography) and MRI (magnetic resonance imaging), allow doctors to obtain detailed three-dimensional images of the patient's body. This helps to diagnose diseases more accurately and plan surgical operations (*Usatiuk, Zhmud, 2018*).

In addition, computer visualization plays a key role in scientific research. It helps scientists model complex natural phenomena such as climate change, the spread of epidemics, or the dynamics of planetary systems. This allows them to gain new knowledge and create innovative solutions to global challenges.

In today's world, the development of artificial intelligence (AI) technologies further expands the capabilities of computer visualization. AI allows automating the analysis of large volumes of images, improving their quality, and creating realistic virtual worlds. As a result, computer visualization is becoming even more effective in various industries, from entertainment to high-tech innovation.

Computer visualization has prospects for rapid development, in particular through the introduction of augmented reality (AR) and virtual reality (VR) technologies. In these environments, users can interact with digital objects in real time, which creates new opportunities for training, education, gaming, design, and even psychological therapy (Fig. 4). For example, architects and engineers can use VR to inspect projects at scale before construction begins, allowing them to identify potential errors at an early stage.

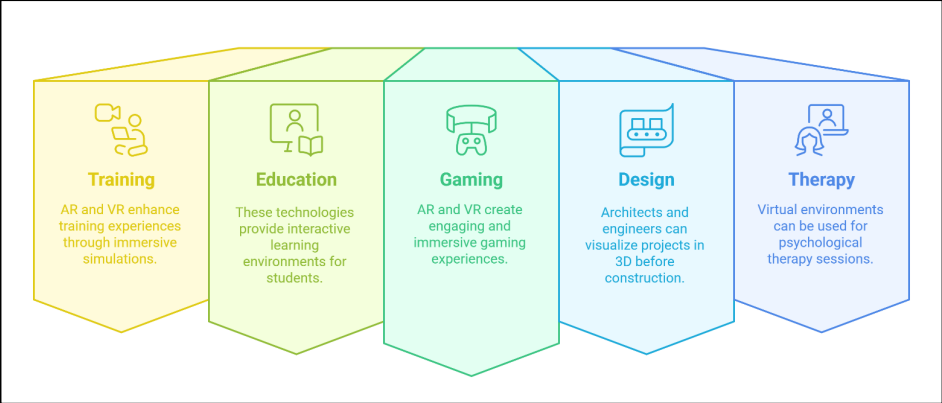


Fig. 4. Application of computer visualization

In cybersecurity and digital forensics, computer visualization helps analyze complex network structures, track threats, and detect anomalies in real time. Visual representation of data flows allows experts to respond faster to cyber threats, optimize system security, and analyze digital traces for investigations (*Kovtaniuk, 2022*).

Another area where visualization is becoming critical is the development of “digital twins.” These are virtual copies of physical objects such as machines, buildings, or even entire cities. They allow you to run simulations, test changes, and analyze the results without risking the real world. Digital twins are actively used in industry, logistics, and urbanism to optimize processes and predict possible problems.

In art and entertainment, visualization opens up unlimited scope for creativity. By combining computer graphics with neural networks, artists create breathtaking digital paintings, animations, and interactive installations. In cinema and video games,

visualization allows viewers to be transported to fantasy worlds with an unprecedented level of detail and realism.

In particular, in the field of social research, computer visualization is becoming a tool for analyzing and predicting the behavior of large groups of people. This is important for modeling urban processes, assessing the impact of political decisions, and even developing strategies for responding to crisis situations such as natural disasters or pandemics (Karakoz, 2023).

Computer visualization continues to integrate into our daily lives through mobile applications, online services, and devices with advanced functionality. For example, visualization technologies are used in personalized medical applications that help users track their health or learn the anatomy of their bodies (Fig. 5).

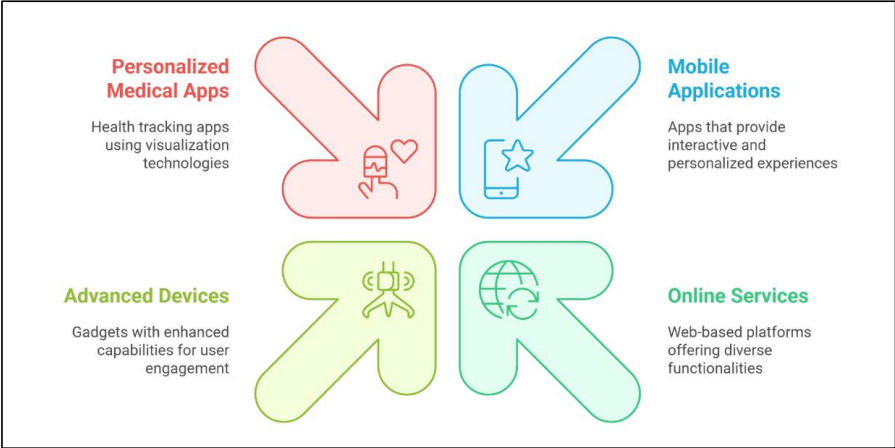


Fig. 5. Integration of computer visualization into everyday life

Computer visualization not only transforms existing industries but also creates new ones, for example, in the field of data and artificial intelligence. Interactive visualizations of big data allow researchers and analysts to interact with information in a convenient format, discover hidden connections, trends, and patterns. This is especially important for making strategic decisions in business, finance, logistics, and risk management.

In the era of smart cities, computer visualization has become a key tool for infrastructure management. For example, digital dashboards allow real-time monitoring of traffic, utilities, air pollution, and much more. This contributes to more efficient use of resources and improves the quality of life for residents (Holub, Kriukova, Kovalenko, 2021).

In the military, visualization provides new opportunities for training and simulation of combat situations. Using virtual and augmented reality simulators, the military can train in a safe environment, practicing strategies and decision-making (Fig. 6). In addition, three-dimensional terrain maps with centimeter-level detail allow for much more accurate planning of operations.

The integration of computer visualization with bioengineering is particularly promising. Real-time visualization of cells, genes, and biological processes opens the door to a more accurate understanding of the nature of life. This can lead to the creation of new medicines, treatment of genetic diseases, and even the cultivation of organs for transplantation.

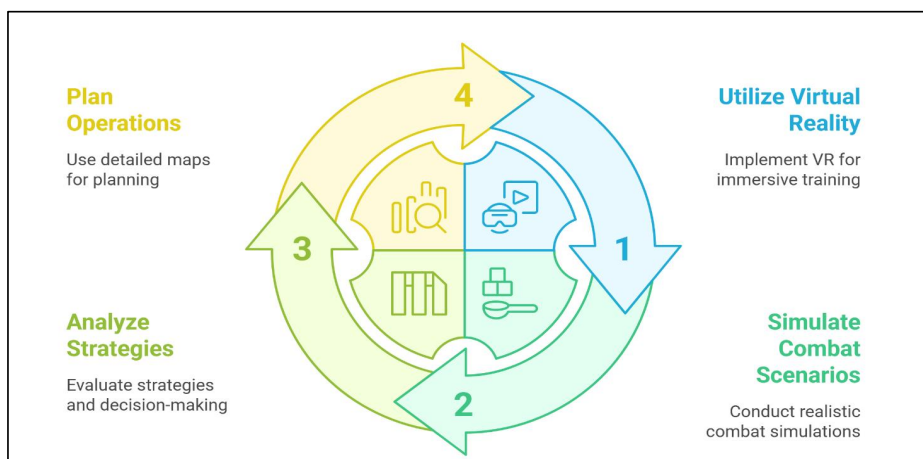


Fig. 6. Military Training Enhancement Cycle

In agriculture, computer visualization allows for optimized crop management. Using drones, satellite imagery, and software, farmers can visually assess soil conditions, plant health, and predict yields. This helps to reduce costs and increase production efficiency (Bondarenko, 2020).

Another area where visualization plays a key role is in ecology and environmental protection. Computer models help reproduce natural systems, analyze the impact of human activity, and predict climate change. Such models enable governments and organizations to develop environmentally sustainable development strategies.

The prospects for computer visualization are also closely linked to the development of quantum computing. The ability to process huge amounts of data and create visualizations of highly complex processes, such as modeling the behavior of elementary particles, can be a real breakthrough in physics, chemistry, and other natural sciences.

Thus, computer visualization is not only a tool for analyzing and presenting information, but also a powerful driver of innovation in many industries. Its future lies in the integration of the latest technologies that will make visualization even more natural, interactive, and accessible (Avramenko, Usatiuk, 2019).

2. Deepfakes and mind manipulation: challenges of computer visualization

The development of computer visualization has significantly expanded the possibilities for creating realistic images and videos. Thanks to deep learning and artificial intelligence algorithms, visual processing technologies have reached a level where digital images are almost indistinguishable from real ones.

One of the most common manifestations of computer visualization is the use of digital facial recognition, a technology that allows you to replace people's faces in a video, change their facial expressions and voice with impressive accuracy.

The development of the technology has both positive and negative aspects. On the positive side, they are used in the film industry, to create special effects and recreate historical events, as well as in education and artificial intelligence training (Kovtaniuk, Titova, 2024).

If we look at the negative side of the equation, they are particularly dangerous in the context of information warfare. After Russia's full-scale invasion of Ukraine, the enemy has

been actively using this technology to spread disinformation and manipulate public opinion. Propaganda materials created with the help of deepfakes often contain shocking content that evokes strong emotions in people, such as panic, fear or anger, which makes it difficult to critically analyze information. In addition, the enemy modifies old photos and videos from the territory of Ukraine to create the impression that they are up-to-date, thus misleading Ukrainian society.

Today, there are many online tools and programs that allow you to create a digital signage even without special knowledge of artificial intelligence. Some of them are based on neural networks, while others use face replacement or voice synthesis algorithms. We will review the most popular services, their capabilities, advantages, and limitations.

StyleGAN or ChatGPT generative models combined with the DALL-E neural network (Fig. 7) allow you to create images that have never existed but look absolutely realistic (Yamkovenko, Kovtaniuk, Kovtaniuk, 2024). Such technologies can be used for both creative and manipulative purposes. In addition, ordinary photo editing with Photoshop or other graphic editors allows you to change the content of images by removing or adding elements that can change the essence of the information conveyed.



Fig. 7. Image generated by the DALL-E neural network with the query "Ukraine's victory in the war against the invader"

Remini is a popular service that uses artificial intelligence technology to enhance (Fig. 8) and create images. It was originally developed as a tool for restoring old or blurry photos, but over time, it has expanded its functionality to include the ability to generate new images (Medvedieva, Titova, 2022).

One of the key features of the service is improving image quality. Remini is able to increase the resolution of photos, eliminate noise and blurring, and add detail. This is especially useful for restoring old or damaged photos, as well as for improving the quality of portraits taken with low-end cameras.

In addition to image enhancement, the service offers the function of generating avatars based on uploaded photos. Users can get images in different artistic styles, such as animated portraits, painting, or digital illustration. This allows you to create unique images that can be used for profiles on social networks or other digital platforms (*Tkachuk, Bondarenko, 2024*).

Another interesting feature is the AI Photo Generator function, which allows you to create images based on a text description or an uploaded photo. Thanks to deep learning algorithms, Remini is able to change facial features, apply stylization to images, and simulate the process of rejuvenation or aging of a person in a photo.

The service is available as a mobile application for iOS and Android. The free version has certain limitations, such as a limited number of treatments per day, watermarks, or ads. To access all the features, you can sign up for a premium subscription, which opens up the possibility of unlimited image generation and enhancement.



Fig. 8. An example of an enhanced photo in the Remini app

Remini remains one of the most popular image manipulation tools thanks to its combination of ease of use and powerful AI algorithms. It is suitable for both ordinary users who want to improve their photos and content creators looking for styling and image generation tools.

Ai Faceswap is a free online service that allows you to quickly and easily replace faces in photos using artificial intelligence. Its main advantage is its ease of use, as it doesn't require registration, software downloads, or complicated settings. All you need to do is upload an image, select a new face, and the neural network will automatically substitute it for the old one (Fig. 9). The process takes a minimum of time, and in a few seconds, you can get the finished result (*Titova, 2024*).

One of the features of the service is the absence of censorship, which means that the user can replace the faces of any people, including famous personalities. This distinguishes it from many similar platforms that have restrictions on the use of celebrity images.

The result of the service is saved in JPEG format with a size of about 232 KB. This means that the photo will have a rather low quality compared to the original (Fig. 10), which can be a disadvantage for those who want to get a high-precision image. However, for entertainment use or quick demonstration of the result, this format is quite suitable.

Ai Faceswap is suitable for those who want to quickly change the face in a photo without too much effort (Fig. 9). It is simple, fast, and requires no special knowledge. At

the same time, the low quality of the output file can be a disadvantage for those who need a more professional result. Nevertheless, the service remains a good tool for fun and experimentation with images (Lytvynova, Kuzminska, Medvedieva, 2022).

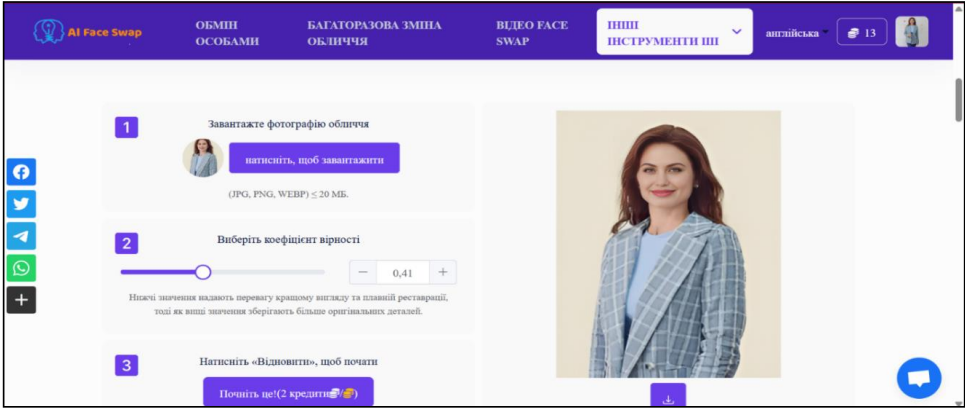


Fig. 9. Face replacement using the online service Ai Faceswap



Fig. 10. The result of the Ai Faceswap service

Vidnoz Face-Swap is an online service for replacing faces in photos and videos using the technology of deepfacing. It allows processing not only static images but also video files, which makes it convenient for creating realistic face replacements in dynamic content. One of the features of the service is its support for multiple deepfakes, which allows you to replace the faces of several people in one frame while maintaining naturalness and high detail.

The service is based on a credit system. Each user receives one free credit, which is enough for one face replacement. In order to download the resulting image or video, you need to be authorized. The free version offers a PNG image of approximately 1 MB in size, which is of high quality but contains a watermark. If the user wants to get a file without a watermark, he or she will have to use additional credits or subscribe (Kruhlyk, Tryhub, Mamonov, 2022).

The service stands out among its peers for its ability to work with video and support for simultaneous processing of several people in a frame, which makes it useful for content creation (Fig. 11), editing materials, or entertainment purposes.

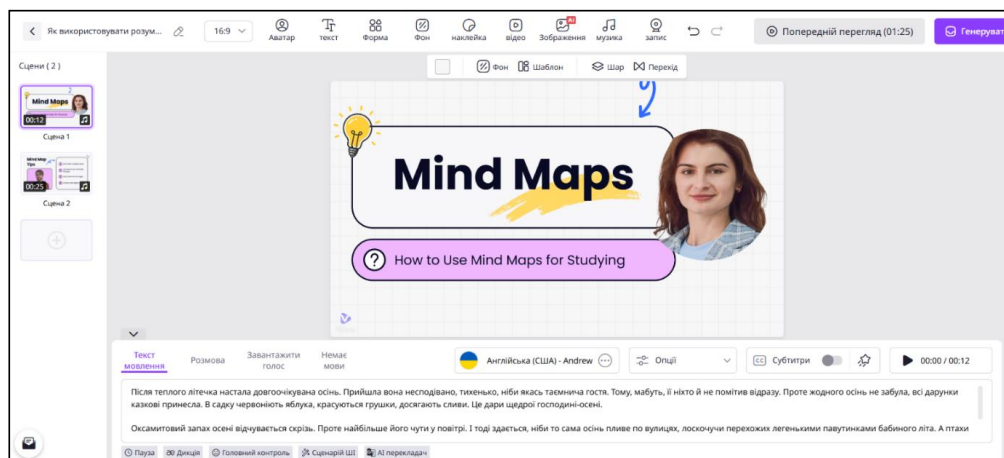


Fig. 11. Creating a video lecture in the Vidnoz Face-Swap service

Face Swap Online Free is a web service that allows you to change faces in photos for free, using artificial intelligence to create realistic and accurate results. The platform works online without the need to install additional software, making it accessible to any user regardless of device.

The main advantage of the service is its simplicity and speed of use. It is enough to upload a photo, select the area to replace the face and add a new image, after which the algorithm will automatically adjust colors, shadows and textures to make the final result look as natural as possible. Thanks to the high-precision technology for recognizing and selecting details, the images are of high quality and realistic (Fig. 12), even without manual adjustment.

The platform is suitable not only for entertainment, but also for professional image editing, as it allows you to fine-tune the face replacement parameters. In some versions of the service, you may be able to edit several faces in one photo, as well as process images with different angles and lighting (Kryvoruchko, 2024).

Among the limitations, it is worth noting that free access may include a watermark on the final image or reduced file quality for saving. Overall, however, Face Swap Online Free is a convenient and affordable tool for quickly swapping faces, suitable for both entertainment and content creation.

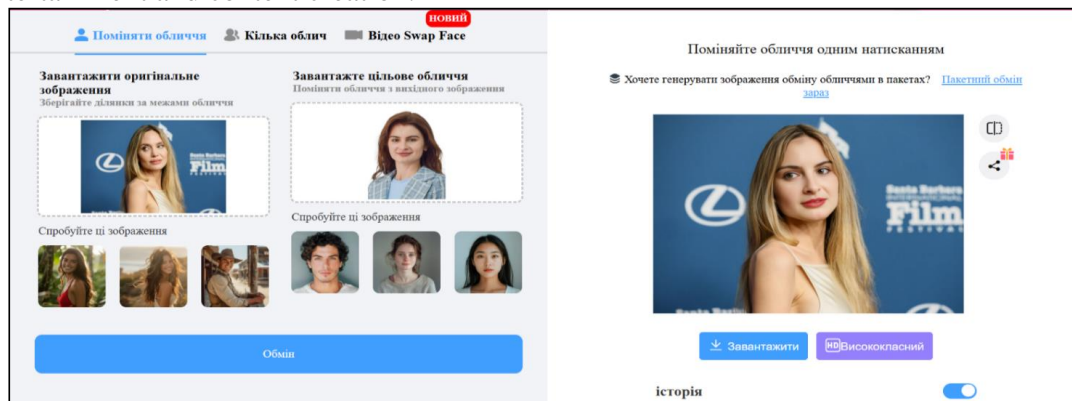


Fig. 12. The result of face replacement in the Face Swap Online Free web service

Faceswapper is a modern platform that uses artificial intelligence to edit images, offering a wide range of tools for manipulating visual content. The main function of the service is to replace faces in photos (Fig. 13) and GIF animations, which allows you to create realistic and dynamic effects without the need for special skills in graphic design.

In addition to the standard face substitution, Faceswapper provides a unique opportunity to change the clothes on a photo, which opens up new horizons for personalizing images. This allows users not only to change faces but also to experiment with style, creating holistic and harmonious images.

The platform is powered by powerful neural network algorithms that ensure high quality processing, natural replacements, and smooth GIF animations. The intuitive interface allows you to quickly upload images, select the necessary effects, and get the finished result without any extra effort. The combination of functionality and ease of use makes Faceswapper the perfect tool for creativity, entertainment, and visual experimentation (*Kryvoruchko, Kovtaniuk, 2022*).

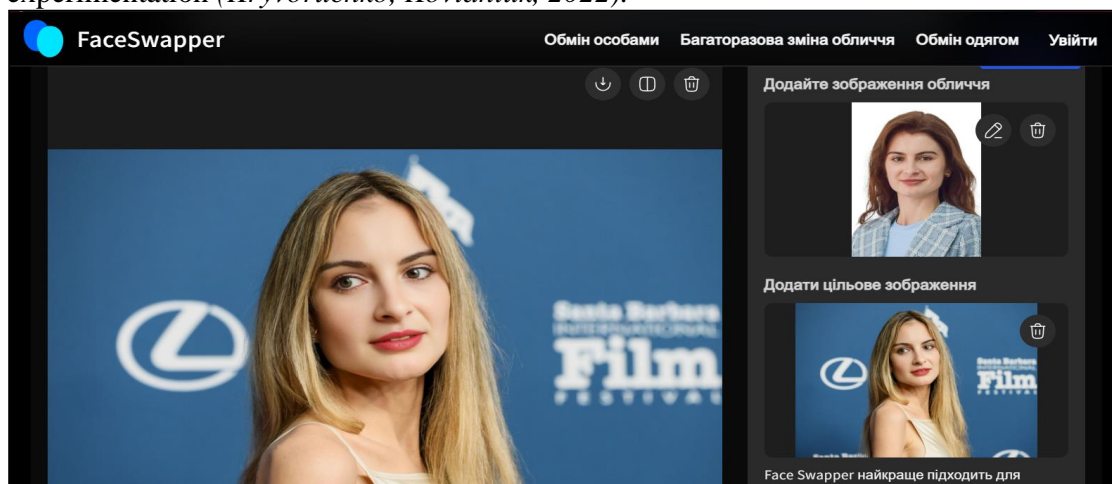


Fig. 13. The result of face replacement in the Faceswapper service

Elai.io is an innovative platform that allows you to create training videos using artificial intelligence, completely eliminating the need for cameras, studios, or green screen. This technology allows you to generate professional videos with virtual presenters in just a few minutes, making the content creation process fast, affordable, and efficient.

The service offers a wide range of avatars – digital presenters who voice text in a realistic and natural way. The user only needs to upload or enter text, and then the neural network will automatically create a video, synchronizing the speech and movements of the virtual presenter (Fig. 14). With support for multiple languages and different voice models, Elai.io is suitable for creating content for a global audience (*Baranetska, 2019*).

The platform's interface is intuitive and does not require special skills in video editing or working with graphic editors. Users can add their own backgrounds, insert images, slides, or text blocks, allowing them to create personalized videos for specific needs – from corporate training to marketing presentations and educational courses.

However, the development of such technologies also raises the issue of deepfakes – videos created with the help of artificial intelligence that can imitate real people. Deepfakes offer great opportunities for creativity and content automation, but also raise concerns about

their potential use in manipulation and disinformation. Elai.io applies ethical approaches to content creation, providing users with legal and transparent tools for video generation. It is important to note that this platform is not intended to create misleading or fraudulent digital avatars. All digital avatars are officially created models, and users cannot replace the faces of real people without their consent.

The platform is an ideal solution for companies, educational institutions, and content makers who want to create high-quality learning materials quickly and efficiently without high production costs. Elai.io greatly simplifies the process of producing video content, making it accessible to anyone who wants to convey information to their audience in a modern format (*Medvedieva, Titova, 2022*).

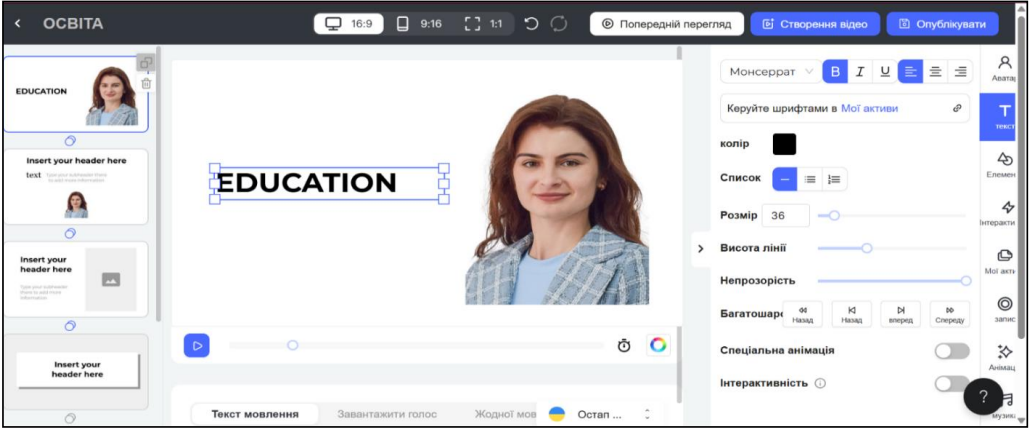


Fig. 14. A digital presenter who reads the text

Consider Canva, one of the most popular online graphic design editors that also has features for creating manipulative images, including digitized images. Although Canva is not a specialized service for creating complex neural network-based dipshots, its capabilities allow users to change faces, edit photos, and create realistic fakes using built-in artificial intelligence tools (Fig. 15).

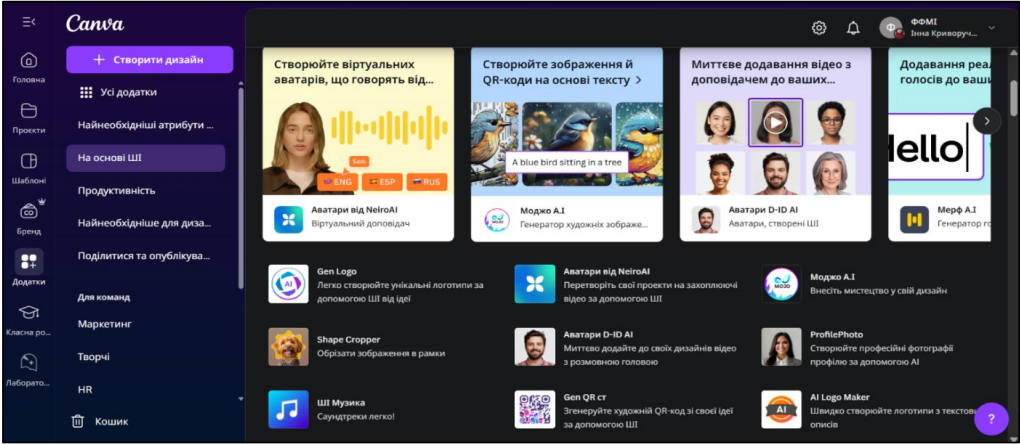


Fig. 15. Applications in the Canva online service based on artificial intelligence

Magic Media in Canva is a powerful AI-powered tool that allows users to create and edit media files, including images and videos. This tool opens up new possibilities for

designers, marketers, and anyone working with visual content by providing simple and intuitive ways to automate creative processes.

One of the main functions of Magic Media is to generate images based on text queries. The user can describe the desired result in a few words or sentences, and artificial intelligence will instantly create the appropriate graphic (Fig. 16). This allows you to quickly get unique illustrations without wasting time searching through photo stocks or drawing them manually. The image generator supports various styles (Fig. 17) and formats, so users can customize the visual design to suit their needs (Kryvoruchko, Titova, 2024).

In addition to creating static images, Magic Media also works with videos. It can edit videos, change their backgrounds, add effects, or even generate new animated scenes based on a text description. This greatly simplifies the process of creating advertising materials, social posts, and presentations.

Another important feature of Magic Media is automatic image quality enhancement. Artificial intelligence algorithms are able to recognize problem areas in photos, eliminate blur, improve colors, and adjust lighting. This is especially useful for those who work with low-quality photos or want to quickly edit images before using them in a project (Kruhlyk, Tryhub, Mamonov, 2022).

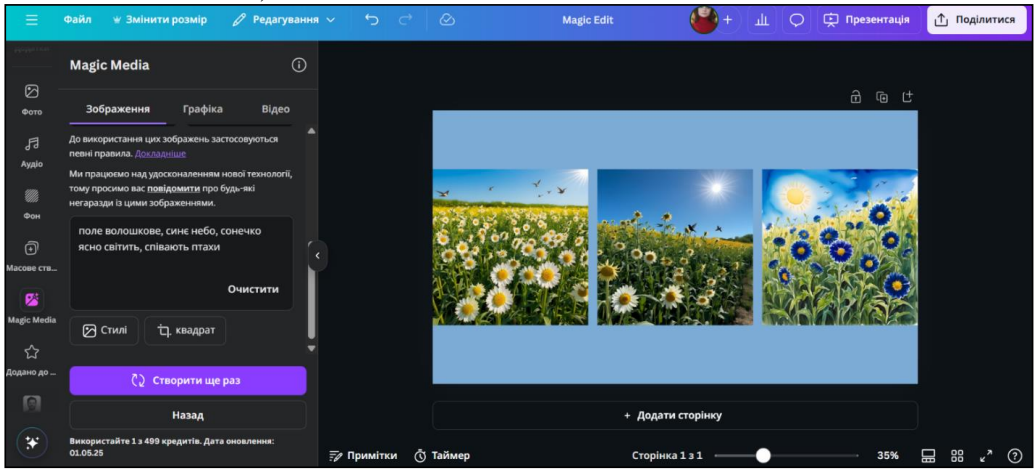


Fig. 16. Generated images for a specific request

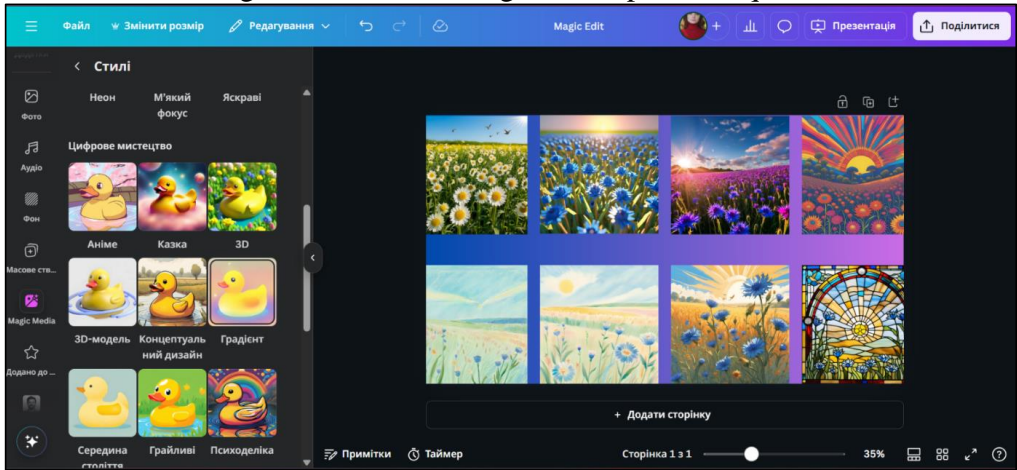


Fig. 17. Different styles of generated image on request

Magic Media can also help with editing faces and objects in images. The user can easily change facial expressions, remove unwanted elements, or adapt the background to a new style. All this happens automatically, without the need for deep knowledge of graphic design.

Thanks to Magic Media's integration into the Canva interface, this tool remains accessible and easy to use even for beginners. All changes are applied in real time, and intuitive settings allow you to quickly get the desired result. Magic Media makes content creation much easier, reducing time spent on mundane tasks and allowing you to focus on your creativity.

With the Canva for Education plan (Kovtaniuk, 2024), users get access to the Background Removal feature for free. This feature is powered by artificial intelligence and allows you to cut an object out of the background very accurately and cleanly with just one click (Fig. 18).

Unlike many other services that leave jagged edges or distorted details after removing the background, Canva's deep learning algorithms carefully determine the boundaries of the object, ensuring maximum clarity and a natural look. Even if the background has complex details or gradients, Canva removes them correctly without unnecessary artifacts.

This is especially useful for creating professional presentations, training materials, or creative projects. Since the feature is available in a free plan for educators and students, it becomes an indispensable tool for those who want to work with high-quality graphics without extra costs and complex editing (Medvedieva, Zhmurko, Kryvoruchko, Kovtaniuk, 2021).

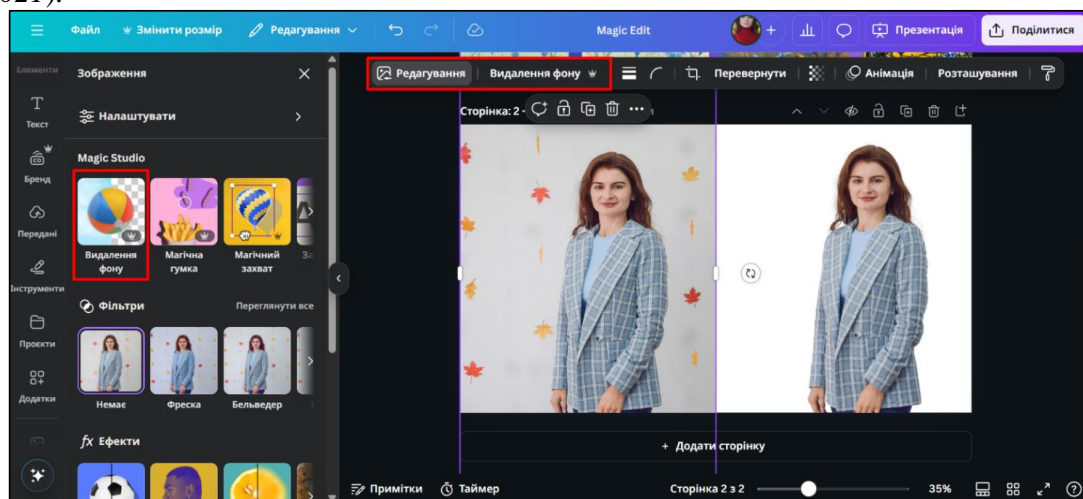


Fig. 18. Remove the background from the image

Canva also has AI image generation (Fig. 19), which allows you to create new faces or modify existing images based on text queries. This feature can be used to generate fake photos, which is potentially misleading if used for manipulative purposes.

Unlike professional services for deepfakes, Canva does not use deep neural networks to replace faces in videos, but its tools can create plausible photo fakes, which also poses a risk. Therefore, the use of such features requires a responsible approach and awareness of the ethical aspects of working with visual content.

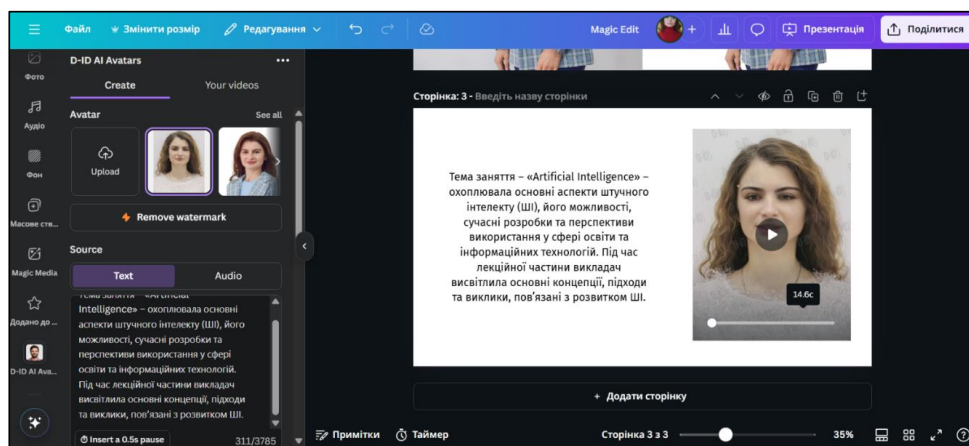


Fig. 19. A video created from a photo using the «D-ID AI Avatars tool»

As for voice diphones, there are specialized services that allow you to clone the voices of famous people or create fully synthetic voices that can imitate real ones.

Retrieval-based Voice Changer (RVC) is an advanced technology based on deep neural networks that allows you to change the voice of one speaker to another person's voice (Fig. 20). It works on the principle of training models on audio recordings, which makes it possible to achieve realistic voice imitation with a minimum amount of input data. The main advantage of this technology is the ability to create high-quality voice dipfaces using only a ten-minute sample of the target person's voice (*Tselik, 2024*).

The RVC system is based on deep neural networks that analyze voice features, including timbre, intonation, and articulation. This allows the model to accurately reproduce the speech characteristics of a particular person and apply them to any other voice recording. The algorithm is based on methods of extracting and transforming acoustic features, which allows synthesizing voice fragments with a natural sound and a high level of authenticity.

RVC technology is used in various fields, including dubbing, voice assistants, and the entertainment industry. It makes it possible to change the voices of actors, synthesize the voices of historical figures, or even create personalized audio messages. At the same time, its use raises ethical and security issues, as it can be used to create unfair fakes. That is why the development of RVC is accompanied by the development of mechanisms for detecting fraud and regulating its use.

OpenAI's Voice Engine is a tool for realistic voice synthesis that can reproduce a human voice based on only a 15-second audio sample and a text input signal (Fig. 21). By using deep neural networks, this technology allows you to accurately reproduce the timbre, intonation, and rhythm of a particular person's speech, creating a natural and authentic sound.

The main feature of Voice Engine is its ability to quickly adapt to new voices, making it an effective solution for various tasks such as automated dubbing, voice assistants, and personalized audio services. However, due to the potential risks associated with voice fraud and possible abuse, OpenAI has limited public access to this technology (*Yamkovenko, 2023*). Currently, it is used only in selected services, including ChatGPT for generating natural voice communication, as well as in cooperation with Spotify for automatic dubbing of podcasts in different languages.

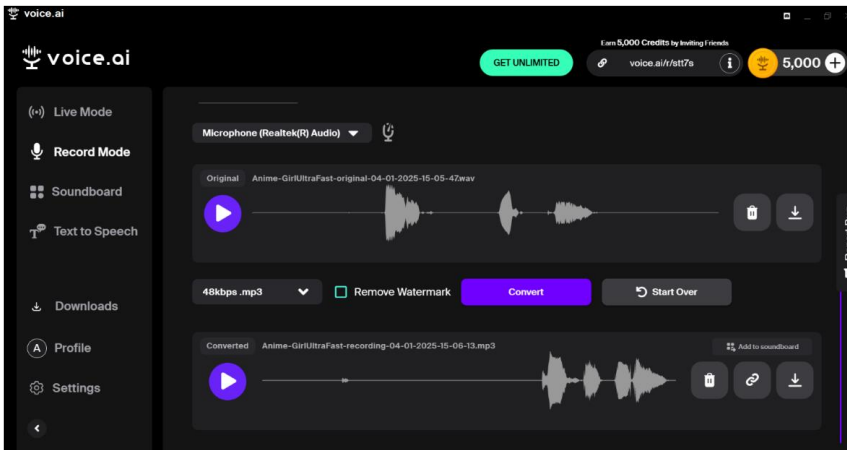


Fig. 20. Replacing the voice of one speaker with the voice of another person in Retrieval-based Voice Changer

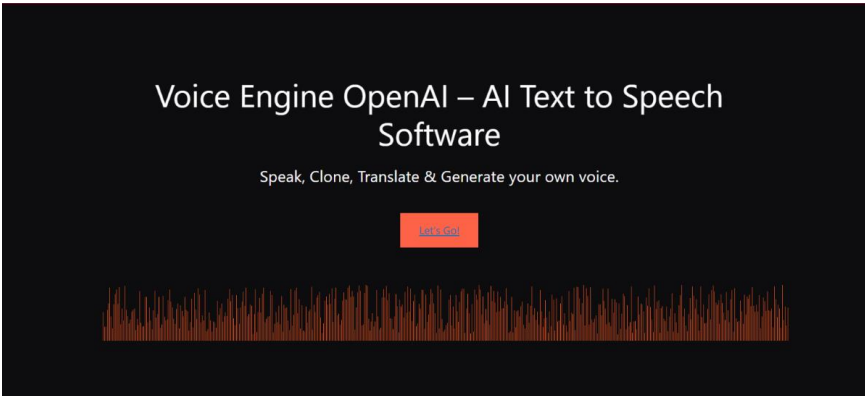


Fig. 21. A tool for realistic voice synthesis Voice Engine by OpenAI

The development of the Voice Engine takes place in the context of growing concerns about the security of voice technologies, so OpenAI focuses on implementing ethical restrictions and mechanisms for identifying synthesized voice. This should ensure responsible use of the technology and prevent its abuse in areas where voice authenticity is critical.

Microsoft's Azure AI Speech Text to Speech Avatar is an innovative feature that allows users to create realistic videos with digital avatars that can voice text scenarios (Fig. 22). This technology combines advanced deep learning algorithms responsible for speech synthesis with animation control models that synchronize facial and lip movements with the voice to provide a natural presentation of information.

To create such an avatar, the user uploads an image of a person, which the system uses to generate a digital model. Next, a text script is entered and processed using highly accurate text-to-speech (TTS) algorithms that support a wide range of languages and voice styles. The model not only generates a synthetic voice, but also analyzes speech characteristics such as tone, pauses, and accents, making speech as natural as possible. At the same time, the system reproduces the corresponding facial expressions, mouth and head movements to create a realistic visualization of speech (Titova, 2024).

With the ability to personalize avatars and customize voice parameters, this technology is used in a variety of industries, including education, marketing, corporate communications, and customer service. Azure AI Speech Text to Speech Avatar allows companies to create interactive presentations, virtual assistants, and training videos without the need for real actors or speakers.

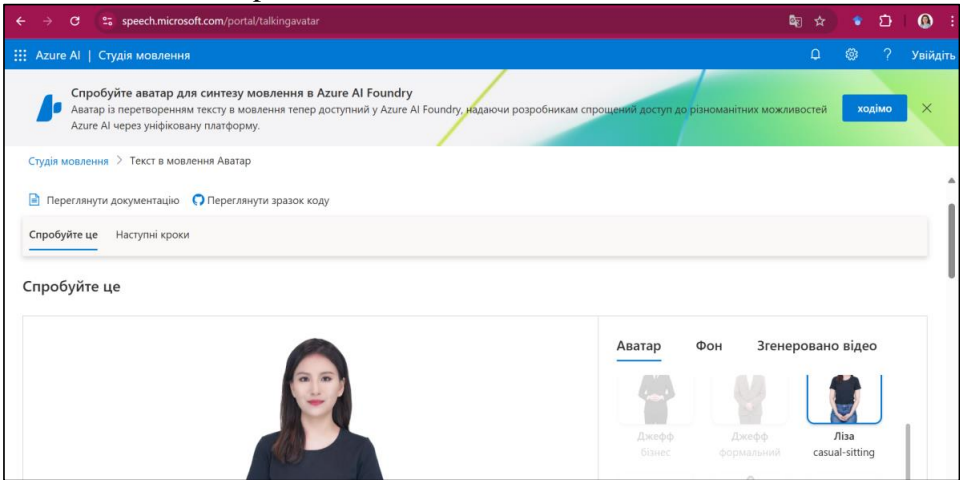


Fig. 22. Create a video with digital avatars using Azure AI Speech Text to Speech Avatar from Microsoft

Microsoft focuses on the ethical use of this technology by introducing restrictions and verification mechanisms to prevent potential misuse. This includes controlling access to avatar creation and the use of watermarks or markers to identify artificially generated content. Thus, Azure AI Speech Text to Speech Avatar combines advanced speech synthesis and animation technologies to provide users with a powerful tool for creating realistic digital representatives.

ElevenLabs is an artificial intelligence service designed to generate audio from text with extremely high quality synthesized voice (Fig. 23). Its technology is based on deep neural networks that analyze natural speech features such as intonation, timbre, pauses, and emotional nuances, which allows you to create the most realistic voice.



Fig. 23. Types of audio generation from text

One of the key advantages of ElevenLabs is its ability to mimic human speech patterns with great accuracy, making it ideal for audiobooks, videos, podcasts, and even interactive applications. Users can choose from a variety of synthetic voices or create personalized models based on specific speech patterns. The system also supports multilingual synthesis, which allows you to generate voice recordings in different languages with natural accents and intonation.

Thanks to its flexible customization options, ElevenLabs allows you to control the emotional tone of the voice, adjust the speed of speech, and adapt the voice to different contexts, such as formal speeches, literary reading, or interactive dialogues. This makes the service a valuable tool for content makers, journalists, educational platforms, and businesses that use voice technologies to automate communications.

The company pays considerable attention to the ethical aspects and security of its technology, implementing mechanisms to protect against abuse, such as limited access to voice cloning functions and verification systems that prevent unauthorized use of voice models. This makes ElevenLabs not only a high-tech, but also a responsible solution in the field of speech synthesis (Kovtaniuk, 2022).

Hume AI is an innovative voice generation tool that is distinguished by its ability to convey a wide range of emotional tones, making synthesized speech more natural and expressive (Fig. 24). Its technology is based on deep neural networks that analyze and reproduce the peculiarities of human emotional communication, providing realistic voice with variable intonation, rhythm, and timbre.

The main advantage of Hume AI is the ability to adapt the voice to the context, conveying emotions such as joy, sadness, surprise, anger, or calmness. This makes it possible to create audio content that evokes a deeper engagement and emotional response from the listener. The technology can be used to dub movies and videos, voice interactive characters, create voice assistants, and generate personalized audio messages that sound as human as possible.

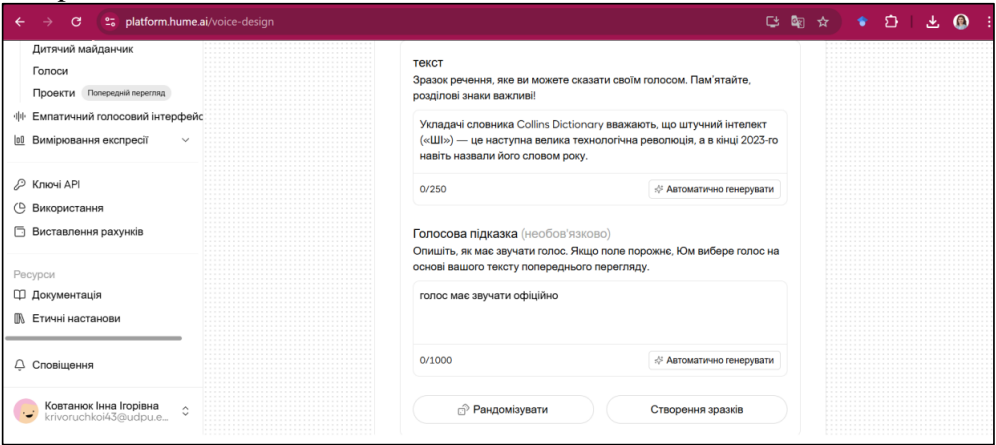


Fig. 24. Hume AI – a tool for voice generation

Hume AI allows users to customize the level of voice expression, adjust the strength of emotional expressions, and experiment with different speech styles. This allows content creators, companies, and developers to create more convincing and engaging voice interfaces. The technology is also used in the field of artificial intelligence research, where

modeling emotions in speech is key to developing more natural and responsive AI systems (*Medvedieva, 2024*).

Hume AI pays special attention to the ethical aspects of using its technology, implementing control and verification mechanisms to prevent potential misuse. The company focuses on ensuring that synthesized voice is used responsibly and contributes to improving the quality of interaction between humans and artificial intelligence.

Despite the fact that services for creating deepfakes are gaining popularity and are constantly improving, this poses serious challenges for ensuring digital security and the veracity of information. Every year, more and more fake videos and images are being posted online, manipulating the perception of events and influencing public opinion. Thus, as technologies for creating fake videos are developing, the demand for services capable of detecting such manipulations is growing. Systems that use artificial intelligence algorithms, machine learning, and other innovative methods have become important tools in the fight against fake content. They help to detect even the most sophisticated spoofs, protecting users from misinformation and falsifications (*Yamkovenko, 2024*).

Among the most famous developments in this area are Microsoft Video Authenticator, Deepware Scanner, and Sensity AI, which can automatically check content for signs of a deepfake.

Microsoft Video Authenticator is a tool developed by Microsoft to authenticate images, videos, and audio files. It uses artificial intelligence to analyze digital materials and determine whether they have been altered or created artificially. The program is able to detect traces of editing, analyze pixel anomalies, and assess the level of manipulation, providing the user with a percentage of the probability of fake.

This tool can work with both static images and real-time video, analyzing it frame by frame. The main goal of Video Authenticator is to identify deep fakes that are actively used to spread disinformation, create fake news, and manipulate social media. It can be used in journalism to verify the authenticity of materials, in cybersecurity to protect against fraud, in the corporate environment to prevent fraud, and even in forensic examinations to assess the authenticity of digital evidence.

However, despite the power of the technology, it does not guarantee one hundred percent accuracy. Deep fakes are constantly being improved, and some sophisticated fake methods may go undetected. In addition, processing such data requires significant computing resources, and the algorithm itself must be regularly updated to remain effective in the fight against the latest manipulation methods. Microsoft Video Authenticator is an important step in the fight against disinformation, but it should be seen as one of the verification tools, not an absolute solution.

Deepware Scanner is a mobile application developed by Deepware that is designed to detect deep fakes in videos and images. It uses machine learning algorithms to identify manipulation of media content and help users recognize potentially fake materials.

The application works by analyzing videos and images, checking them for digital anomalies that usually remain after deep learning algorithms are used to create fake content. Deepware Scanner is able to recognize the characteristic defects of deep fakes, such as unnatural eye movements, incorrect shadows, distortion of skin textures, or anomalies in lip synchronization with the voice.

The main feature of Deepware Scanner is its accessibility for users. It offers an easy way to check videos without the need for deep technical knowledge. Users can upload a video file or paste a link to an online video, and the program analyzes it and gives a result with a level of suspicion.

This tool is especially useful on social media, where deep fakes are used to spread disinformation, manipulation, and blackmail. Journalists, researchers, and ordinary users can use Deepware Scanner to check suspicious content before it is shared.

However, like most similar solutions, Deepware Scanner does not guarantee absolute accuracy. Some complex falsifications may go undetected, and the results of the analysis should be taken as an additional level of verification, not a final conclusion. In addition, the tool needs to be constantly updated to adapt to new methods of creating deepfake content.

Despite these limitations, Deepware Scanner is a useful solution for combating digital fakes and increasing media literacy (*Kryvoruchko, 2024*).

Sensity AI is a company that specializes in detecting and analyzing deep fakes, as well as protecting against digital manipulation and cyber threats. It uses advanced artificial intelligence, machine learning, and computer vision algorithms to identify fake videos, images, and audio files. Sensity AI technology works in real time, analyzing large amounts of data and identifying potential threats.

This platform is actively used in various fields such as cybersecurity, media, finance, law enforcement, and the corporate sector. It helps to combat disinformation, digital fraud, and manipulative content that can be used for blackmail, financial fraud, or undermining trust in public institutions. Sensity AI is also capable of analyzing audio recordings and detecting fake voice messages, which is an important tool in financial institutions and legal processes.

The company offers analytical solutions that can integrate with existing security systems to help organizations quickly identify and block threats. Its technology is constantly being updated to meet the challenges posed by the latest deepfake manipulation techniques. Despite their effectiveness, even such advanced systems cannot guarantee one hundred percent protection, as deep fake technologies are evolving rapidly. Sensity AI continues to improve its algorithms to remain one of the leading solutions in the fight against digital threats.

Digital watermarks and content verification technologies are also being actively implemented. For example, Adobe, together with partners, is developing the Content Authenticity Initiative (CAI) standard, which allows embedding metadata confirming their authenticity in digital images and videos. This helps to track the history of changes in a file and detect manipulations. Similar approaches are also used in blockchain technologies, where the history of each media file is recorded, making it more difficult to fake (*Titova, Kryvoruchko, 2024*).

An important area is to increase the level of media literacy among the population. Since even the most advanced recognition algorithms cannot guarantee 100% protection against manipulation, people must learn to critically evaluate content. Media literacy education programs teach people to check information sources, analyze the context of images, and use fact-checking tools. For example, to check photos, you can use Google Reverse Image Search, TinEye, which allow you to find the original photo and determine whether it has been altered.

Another important approach is to create legal and regulatory mechanisms to regulate deepfakes. Some countries have already introduced legislative initiatives that provide for liability for the distribution of malicious deepfakes. For example, the United States has passed laws criminalizing the use of deepfakes for disinformation in election campaigns or cybercrime. Such initiatives are aimed at limiting the use of this technology for malicious purposes.

Social platforms also play a key role in the fight against manipulation. Large companies such as Facebook, Twitter, and YouTube are implementing automatic labeling of potentially fake content and removing dangerous dipshits that can mislead users.

Thus, the fight against dipfakes requires a comprehensive approach, including the use of technological tools, the development of critical thinking among users, strengthening legislative control and the responsibility of digital platforms. Only a combination of these methods will effectively reduce the impact of manipulative content on society.

Conclusions. In today's digital world, digital technologies are rapidly evolving and becoming more accessible to the general public. This opens up great opportunities for creativity, art, advertising, cinema, and even educational projects. However, this also poses a significant threat: the use of diphones to manipulate public opinion, create fake news, fake videos and images that can influence politics, the reputation of individuals, and social processes in general.

One of the main problems with fake news is that it has become so realistic that even experienced users sometimes cannot distinguish between fake and real content. This creates the ground for disinformation, manipulation, and cybercrime. As a result, a person who lacks critical thinking skills and media literacy can easily become a victim of information attacks (Tkachuk, Bondarenko, 2024).

That is why it is important not only to understand the capabilities of these technologies, but also to learn how to identify their manipulative aspects. A modern media user should be able to analyze content, pay attention to its sources, check the accuracy of information, and use tools to recognize fakes.

One of the key aspects of the fight against fake news is the development of critical thinking. People should question overly emotional or sensationalized content, verify information through several independent sources, and use special services that help identify fakes. In addition, at the societal level, it is important to implement media literacy education programs to help people better navigate the digital space.

Thus, while dipshares can be a powerful tool for creative and entertainment purposes, they also pose a significant threat to society if used for manipulative purposes. Therefore, it is necessary to raise the level of media literacy, foster a culture of critical thinking, and learn to consume information responsibly in the digital age. This is the only way to minimize the negative effects of the use of deepfake technologies and effectively counteract the spread of disinformation.

References:

- Kovtaniuk I. I. Innovative features of the Canva online service. Learning & Teaching: *In the World after the War* : III International Scientific & Practical Conference, Kharkiv, 08 November 2024. Kharkiv, 2024. P. 92. URL: <https://dspace.udpu.edu.ua/handle/123456789/17456/>
- Medvedieva M., Titova L. Means of gamification in the formation of media literacy as an element of information and digital competence of participants in the educational process. Information technologies

- and management in higher education and science : International scientific conference. 28 November 2022. Ferghana, Republic of Uzbekistan, P. 294–297. URL: <https://doi.org/10.30525/978-9934-26-277-7-163>.
- Titova L. Digital tools as a means of organizing and controlling the independent work of future mathematics teachers. *Innovations in Education of the Future: Integration of Humanities, Engineering and Natural Sciences* : international collective monograph. Praga, 2023. P. 619–640. URL: <https://doi.org/10.5281/zenodo.10261713>.
- Titova L. O., Kryvoruchko I. I. Cloud services as a means of gamification in the training of future teachers. *Збірник наукових праць «Information Technologies in Education» (ITE)*. 2024. № 56. С. 6–13. URL: <https://doi.org/10.14308/ite000783>.
- Авраменко О. Б., Усатюк Я. В. Теоретичні та методичні проблеми формування медіакомпетентності сучасного педагога. *Наукові записки*. 2019. Вип. CXXXIV (144). С. 5–15. URL: <https://dspace.udpu.edu.ua/handle/123456789/12637>.
- Баранецька А. Д. Візуалізація інформації як складник наповнення медіаконтенту. *Держава та регіони. Серія: Соціальні комунікації*. 2019. № 3 (39). С. 13–17. URL: http://nbuv.gov.ua/UJRN/drsk_2019_3_5.
- Бондаренко Т. Освітні можливості використання геоінформаційних ресурсів Google в процесі візуалізації навчальної інформації. *Інформаційні технології і засоби навчання*. 2020. Том 76. № 2, С. 96–107. URL: <https://dspace.udpu.edu.ua/handle/123456789/12345>.
- Голуб Т. П., Крюкова Є. С., Коваленко О. О. Сучасні технології візуалізації навчальної інформації. *Інноваційна педагогіка*. Випуск 32. Т. 2. 2021. С. 174–177. URL: <https://doi.org/10.32843/2663-6085/2021/32-2.34>.
- Каракоз О. Візуалізація інформації у сучасному освітньому просторі. *Grail of Science*. 2023. № 24. С. 800–803. URL: <https://doi.org/10.36074/grail-of-science.17.02.2023.149>.
- Ковтанюк І. І., Ковтанюк М. С. Canva: від документа до презентації одним кліком. *III Шкловські читання «Проблеми сучасних природничо-математичних наук та методик їх викладання»* : III Всеукр. науково-практ. інтернет-конф. з міжнар. участю, м. Глухів, 30–31 жовт. 2024 р. Глухів, 2024. С. 221–222. URL: <https://dspace.udpu.edu.ua/handle/123456789/17262>.
- Ковтанюк І. І., Тітова Л. О. Критичне мислення в епоху інформаційного шуму: як розпізнавати фейки та маніпуляції в соціальних мережах. *New Horizons in Scientific Research: Challenges and Solutions* : Міжнародна науково-практична конференція, Марсель, 21–23 жовтня 2024 р. Марсель, 2024. С. 127–128. URL: <https://dspace.udpu.edu.ua/handle/123456789/17267>.
- Ковтанюк М. С. Створення мапи думок за допомогою вебресурсу Canva. *Комп'ютерні технології: інновації, проблеми, рішення* : тези доп. V Всеукр. наук.-техн. конф., м. Житомир, 01–02 грудня 2022 р. Житомир, 2022. С. 292–293. URL: <https://dspace.udpu.edu.ua/handle/123456789/15370>.
- Комп'ютерна графіка та мультимедіа. Медіадрайвер: навч.-метод. посібник / МОН України, Уманський держ. пед. ун-т. імені Павла Тичини; уклад.: Усатюк Я. В., Жмуд О. В. Умань: Візаві. 2018. 191 с. URL: <https://dspace.udpu.edu.ua/handle/6789/9701>.
- Криворучко І. І. Storyset як засіб пошуку візуального контенту. *Комп'ютерні технології: інновації, проблеми, рішення* : тези доп. V Всеукр. наук.-техн. конф., м. Житомир, 01–02 грудня 2022 р. Житомир, 2022. С. 296–297. URL: <https://dspace.udpu.edu.ua/handle/123456789/15368>.
- Криворучко І. І. Корисні вебресурси для оформлення навчального контенту. *Наука. Освіта. Молодь* : матеріали XV Всеукр. наук. конф. студентів та молодих науковців, м. Умань, 25 травня 2022 р. Умань, 2022. С. 228–230. URL: <https://dspace.udpu.edu.ua/handle/123456789/14745>.
- Криворучко І. І. Роль графічного дизайну в підготовці навчальних матеріалів майбутніми вчителями інформатики. *Наука і техніка сьогодні*. 2024. № 5(33) 2024. С. 677–687. DOI: [https://doi.org/10.52058/2786-6025-2024-5\(33\)-677-687](https://doi.org/10.52058/2786-6025-2024-5(33)-677-687).
- Криворучко І. І., Аллакулієв К. Використання засобів комп'ютерної візуалізації для формування дослідницької компетентності учнів. *Сучасні інформаційні технології в освіті і науці* : матеріали V Всеукр. наук.-практ. конф., м. Умань, 16–17 лист. 2023 р. Умань, 2023. С. 69–71. URL: <https://dspace.udpu.edu.ua/handle/123456789/16030>.

- Криворучко І. І., Ковтанюк М. С. Вебресурси для створення креативних презентацій. *Сучасні інформаційні технології в освіті і науці* : XIII Всеукр. наук.-практ. конф. для молодих учених та студентів, м. Умань, 19–20 травня 2022 р. Умань, 2022. С. 143–144. URL: <https://dspace.udpu.edu.ua/handle/123456789/15752>.
- Криворучко І. І., Ковтанюк М. С. Медіаграмотність у сучасному світі: захист від дезінформації та виклики дипфейків. *Штучний інтелект у науці та освіті (AISE 2024)* : зб. матер. Міжнар. наук. конф., м. Полтава, 01–02 берез. 2024 р. Київ, 2024. С. 129–131. URL: <https://dspace.udpu.edu.ua/handle/123456789/16767>.
- Криворучко І. І., Тітова Л. О. Хмарні та мобільні технології у підготовці майбутнього вчителя. *Педагогічна академія: наукові записки*. 2024. № 10. DOI: <https://doi.org/10.5281/zenodo.13924205>.
- Круглик К. П., Тригуб І. С., Мамонов М. А. Проектна компетентність як одна з провідних якостей сучасного фахівця. *Мехатронні системи: інновації та інжиніринг* : тези доповідей VI Міжнародної науково-практичної конференції, м. Київ, 24 листопада 2022 року. Київ : КНУТД, 2022. С. 183–184. URL: <https://er.knutd.edu.ua/handle/123456789/20977>.
- Литвинова С. Г., Кузьмінська О. Г., Медведєва М. О. Хмаро орієнтовані технології вчителя інформатики: посібник. Київ: ЦО НАПН України, 2022. 236 с. URL: <https://dspace.udpu.edu.ua/handle/123456789/16577>.
- Медведєва М. О. Медіаграмотність для освітян : навч. посіб. Умань : Візаві, 2020. 118 с. URL: <https://dspace.udpu.edu.ua/handle/123456789/16057>.
- Медведєва М. О., Жмурко О. І., Криворучко І. І., Ковтанюк М. С. Організація продуктивної взаємодії між учасниками освітнього процесу в умовах дистанційного навчання: аналіз сучасних додатків. *Науковий часопис*. 2021. Т. 1, № 80. С. 248–255. URL: <https://dspace.udpu.edu.ua/handle/123456789/13778>.
- Медведєва М.О., Тітова Л.О., Ковтанюк І.І. Цифрові інструменти у формуванні інформаційно-цифрової компетентності здобувачів освіти. *Українські студії в європейському контексті*. 2024. № 9. С. 184–190. URL: <https://dspace.udpu.edu.ua/handle/123456789/17468>.
- Медіаграмотність. Критичне мислення на уроках інформатики: навч.-метод. посібник / уклад.: Усатюк Я.В. Умань: Візаві. 2019. 128 с. URL: <https://dspace.udpu.edu.ua/handle/123456789/11456>.
- Медіаосвіта та медіаграмотність: навч.-метод. посіб. / МОН України, Уманський держ. пед. ун-т імені Павла Тичини ; уклад. В. О. Мельничук. Умань : Візаві, 2023. 123 с. URL: <https://dspace.udpu.edu.ua/handle/123456789/16637>.
- Муковіз О., Мельничук В. Шляхи формування основ медіаграмотності в молодших школярів на уроках інформатики. *Психолого-педагогічні проблеми сучасної школи*. Умань, 2023. №1 (9). С. 111–120. URL: <https://dspace.udpu.edu.ua/handle/123456789/17960>.
- Петько С. М. Особливості використання технологій ІІІ в освітньому процесі. *Імперативи економічного зростання в контексті реалізації Глобальних цілей сталого розвитку* : матеріали V Міжнародної науково-практичної Інтернет-конференції, м. Київ, 23 квітня 2024 року. Київ : КНУТД, 2024. С. 342–347. URL: <https://er.knutd.edu.ua/handle/123456789/27166>.
- Тітова Л. О. Wepik як засіб створення візуального контенту. *Наука. Освіта. Молодь* : XVII Всеукр. наук. конф. студентів та молодих науковців, м. Умань, 30 квіт. 2024 р. Умань, 2024. С. 225–228. URL: <https://dspace.udpu.edu.ua/handle/123456789/16837>.
- Тітова Л. О. Добір сервісів на основі штучного інтелекту для створення візуального навчального контенту. *International Science Journal of Education & Linguistics*. 2024. № 2, т. 3. С. 114–125. URL: <https://doi.org/10.46299/j.isjel.20240302.13>.
- Тітова Л. О. Можливості Slidesgo у створенні візуального навчального контенту. *Штучний інтелект у науці та освіті (AISE 2024)* : зб. матер. Міжнар. наук. конф., м. Київ, 01–02 берез. 2024 р. Київ, 2024. С. 274–276. URL: <https://dspace.udpu.edu.ua/handle/123456789/16785>.
- Тітова Л. О., Ковтанюк М. С., Ямковенко В. О. Цифрові засоби розвитку медіаграмотності здобувачів освіти. *Українські студії в європейському контексті*. 2024. № 8. С. 305–311. URL: http://obrii.org.ua/usec/storage/conference/zb_vol8_2024.pdf.

- Ткачук Г. В., Бондаренко Т. В. Можливості систем штучного інтелекту в роботі учасників освітнього процесу. *Світові освітні тренди: навчання впродовж життя в інформаційному суспільстві* : матеріали Міжнародної науково-практичної конференції присвяченої 190-річчю Університету та 50-річчю Інституту, м. Київ, 20-21 червня 2024 року. Київ. 2024. С. 212–214. URL: <https://dspace.udpu.edu.ua/handle/123456789/17724>.
- Целік Н. С. Цифрові технології в науці та освіті: потенціал хмарних сервісів для євроінтеграції. *Історія науки – майбутньому вчителі ' 2024 «Становлення та розвиток науки на теренах незалежної України»* : збірник матеріалів Всеукр. студ. наук.-практ. конф., м. Умань, 18 квіт. 2024 р. Умань, 2024. С. 110–112. URL: <https://dspace.udpu.edu.ua/handle/123456789/16771>.
- Штаєр Р. В., Назаров В. С., Кравець О. В. Можливості використання інформаційних технологій в освітньому процесі. *Науковий вісник Ужгородського університету : серія: Педагогіка. Соціальна робота*. Ужгород : Говерла, 2023. Вип. 2 (53). С. 156–160. с. 159. URL: <https://dspace.uzhnu.edu.ua/jspui/handle/lib/56348>.
- Ямковенко В. О. Інформаційна грамотність здобувачів освіти як навичка XXI століття. *Глухівські наукові читання – 2023. Актуальні питання суспільних та гуманітарних наук* : зб. матеріалів XII Міжн. інтернет-конф. для молодих уч. і студентів, м. Умань, 6–8 груд. 2023 р. Глухів, 2023. С. 28–30. URL: <https://dspace.udpu.edu.ua/handle/123456789/15979>.
- Ямковенко В. О., Ковтанюк І. І., Ковтанюк М. С. Використання онлайн-сервісів на основі штучного інтелекту для створення навчальних матеріалів з інформатики. *Scientific Research: Modern Innovations and Future Perspectives* : III-я Міжнародна науково-практична конференція, м. Монреаль, 24–26 лютого 2025 р. Монреаль, 2025. С. 237–239. URL: <https://dspace.udpu.edu.ua/handle/123456789/18105>.
- Ямковенко В. О., Тітова Л. О. Сервіси для роботи з графічними зображеннями на базі штучного інтелекту. *Наука. Освіта. Молодь* : XVI Всеукр. наук. конф. студентів та молодих науковців, м. Умань, 11 травня 2023 р. Умань, 2023. С. 393–395. URL: <https://dspace.udpu.edu.ua/handle/123456789/15463>.

CHAPTER 15.

INTERCULTURAL COMMUNICATION IN INFORMATION SECURITY: RISKS, CONFLICTS, AND EDUCATIONAL OPPORTUNITIES FOR ENGLISH LANGUAGE TEACHERS

Svitlana NYKYPORETS

senior English language lecturer

Vinnitsia National Technical University,

Department of Foreign Languages,

(95, Khmelnytske shose, Vinnitsia, 21021, Ukraine)

fotinia606@gmail.com

<https://orcid.org/0000-0002-3546-1734>

Halyna KUKHARCHUK

English language lecturer

Vinnitsia National Technical University,

Department of Foreign Languages,

(95, Khmelnytske shose, Vinnitsia, 21021, Ukraine)

galinakuh07@gmail.com

<https://orcid.org/0009-0003-7877-1921>

Abstract. This study addresses the urgent challenge of intercultural miscommunication in the context of international security, emphasising how cultural and linguistic biases can heighten the risks and consequences of conflicts such as the ongoing Russian-Ukrainian war of aggression. It examines the complex ways in which values, social norms, and language use shape how information is transmitted and received. Through analysing both historical and contemporary instances of misinterpretation, the research highlights the impact of disinformation and the need for culturally informed strategies to prevent escalation. It proposes a model for integrating intercultural communication competences into English language curricula, based on empirical evidence gathered in Ukrainian educational settings. The findings indicate that incorporating authentic materials, real-world simulations, and critical discussions on global issues can significantly enhance learners' cultural awareness. Moreover, the study reveals that strengthening intercultural competences fosters greater resilience and collaboration in times of geopolitical turmoil. Recommendations are provided for educators and policymakers to design programmes that bridge linguistic, cultural, and civic knowledge in a way that benefits communities facing complex socio-political challenges. Case studies demonstrate that students who receive methodical intercultural training are better equipped to identify and counteract manipulative information campaigns. Ultimately, the research advocates for a proactive, context-sensitive approach to language teaching, which aligns with Ukraine's broader pursuit of peace, stability, and international dialogue. By situating English instruction within a nuanced understanding of global cultural dynamics, the study affirms the vital role educators and linguists can play in bolstering national and international security efforts.

Key words: intercultural communication, disinformation, information security, English language teaching, critical thinking.

In an increasingly interconnected world, where digital communication transcends borders and cultures, information security has become a critical priority. This global reliance on information technology has brought both opportunities and challenges, particularly in maintaining the confidentiality, integrity, and availability of information. Among the myriad factors influencing information security, the role of language – specifically English – stands out as a critical yet underexplored domain. English has firmly established itself as the *lingua franca* of global business, diplomacy, technology, and cybersecurity, making its linguistic and sociolinguistic aspects an essential component in understanding and addressing security concerns.

The significance of linguistic perspectives in information security lies in their ability to unveil the nuanced ways in which language shapes, conveys, and sometimes compromises information. From the terminologies used in coding and encryption to the protocols for international communication and the wording of security warnings, the linguistic dimension influences both technical processes and user interactions. Miscommunication or ambiguous language, for instance, can lead to vulnerabilities that malicious actors might exploit, highlighting the critical need for precise and universally comprehensible terminologies. Furthermore, the cultural and contextual implications of language must also be considered, as differences in linguistic norms can lead to variations in how security measures are understood and implemented across regions.

The role of English in this landscape is particularly noteworthy. As the primary medium of communication in international cybersecurity initiatives, technical documentation, and policy formulation, English has become the *de facto* standard for sharing knowledge and fostering collaboration. However, this dominance also introduces challenges, particularly for non-native English speakers, who may struggle with the technical jargon and nuanced phrasing that often characterize the field. These linguistic barriers can hinder effective communication, contribute to misinterpretations, and exacerbate global disparities in cybersecurity readiness.

At the heart of these challenges lies a pressing question: How can the global community leverage the linguistic dominance of English while mitigating its potential drawbacks? This question extends beyond the technical realm, touching on issues of linguistic inclusivity, equity, and the ethical considerations of a linguistically diverse world. Addressing this question requires an interdisciplinary approach, combining insights from linguistics, information technology, and global governance.

This article explores the intersection of linguistics and information security, with a particular focus on the role of English as a medium for global cybersecurity communication. By examining how linguistic factors influence information security practices and outcomes, it aims to provide a deeper understanding of the ways language shapes the security landscape. Key areas of focus include the implications of linguistic precision in technical documentation, the challenges of multilingual communication in international cybersecurity efforts, and the strategies for overcoming linguistic barriers to foster inclusivity and collaboration.

The discussion will also delve into the potential for linguistic analysis to uncover patterns and vulnerabilities in cybercriminal activity, shedding light on the critical role of language in both the offensive and defensive dimensions of cybersecurity. By bringing linguistic perspectives into the conversation, this article seeks to bridge the gap between

language and technology, offering insights that are both academically enriching and practically relevant in addressing the global challenge of information security.

In a world where information is both a resource and a target, the interplay between language and security cannot be overlooked. As this article demonstrates, understanding and addressing the linguistic dimensions of information security are essential steps toward creating a safer, more inclusive, and better-informed global community. English, as a pivotal player in this dynamic, holds both the potential to unify and the risk of dividing – depending on how its role is navigated. This exploration invites readers to consider not only the technical but also the human aspects of cybersecurity, urging a more holistic and linguistically aware approach to tackling one of the most pressing challenges of our time.

I. Risks of misinterpreting information in a multicultural environment

1. Introduction to the issue of misinterpretation

In today's globalized society, communication is more rapid, extensive, and diverse than ever before. Technological advancements have paved the way for instantaneous interactions across continents, fostering the creation of multicultural environments in which people from varied linguistic and cultural backgrounds engage. However, as much as these developments connect us, they also introduce significant challenges, particularly regarding the accurate interpretation of information.

Misinterpretation, in the context of communication, can be broadly defined as the failure to understand a message, statement, or piece of information in the way it was originally intended. This failure often arises (*Paxton, 2021*) from linguistic ambiguity, cultural differences, or cognitive biases. It is essential to note that misinterpretation is not necessarily the result of one party's lack of proficiency in a language; rather, it can stem from subtle mismatches between language, intent, and perception – factors that become even more pronounced in multicultural settings.

A multicultural environment, in this discussion, refers to any space – physical or virtual – where individuals from diverse cultural, linguistic, and social backgrounds interact. Such environments could be international workplaces, global educational institutions, online forums, diplomatic platforms, or multinational corporations. Within these spaces, participants bring their own cultural assumptions, communication styles, and linguistic conventions to the table. While diversity can foster creativity and innovation, it can also heighten the likelihood of misunderstandings if cultural cues and context are not properly accounted for.

The importance of context and cultural differences in communication cannot be overstated. Language often reflects deeply embedded cultural norms, values, and beliefs that shape how people interpret words, gestures, and symbols. For example, some cultures place great emphasis on indirect communication to maintain social harmony, while others value directness and clarity. These cultural norms, when overlooked, can cause significant confusion. Similarly, context – be it social, historical, or situational – provides critical cues for correctly decoding messages. Without adequate contextual knowledge, even well-intentioned communicators may be misunderstood, resulting in mistakes that range from minor social faux pas to severe diplomatic or security breaches.

Analysis of the latest research and publications addressing the problem

Over the past decade, the scholarly community has increasingly acknowledged the profound impact of intercultural communication on information sharing and security.

Researchers have underscored that in a globalised environment – where diverse cultural norms, values, and linguistic repertoires intersect – misinterpretation is not just a theoretical issue but a tangible threat to cooperation, social cohesion, and crisis response. This line of inquiry has further intensified following geopolitical upheavals worldwide, including the ongoing Russian-Ukrainian war of aggression, which has laid bare the immense consequences of communicative breakdowns and the urgent need for effective intercultural strategies.

One of the foundational contributions to this domain comes from Michael Byram, whose work *Teaching and Assessing Intercultural Communicative Competence* (Byram, 2020) has provided a systematic framework for embedding cultural awareness in language education. Byram's concept of "savoirs" – knowledge, skills, and attitudes – continues to inform how educators design programmes aiming to cultivate open-mindedness and reduce cultural bias. While he does not specifically address the war in Ukraine, his paradigm has been adapted by other researchers to examine how misinterpretation can exacerbate tensions in conflict-prone regions.

Building on these insights, Claire Kramsch has contributed significantly to understanding the symbolic and power-laden facets of language. In her more recent publication, *Language as Symbolic Power* (Kramsch, 2021), Kramsch explores how linguistic practices encode ideologies that can either facilitate or obstruct genuine dialogue. Although her focus is often on classroom interaction, her arguments about how language choices and cultural frames shape perceptions of authority bear special relevance when countries such as Ukraine must communicate their positions on sovereignty and security to diverse international audiences.

Within the sphere of Global Englishes, Jennifer Jenkins (Jenkins, 2015) has offered a comprehensive overview of how English adapts to multilingual and multicultural contexts. Her discussion of "lingua franca" communication emphasises intelligibility over native-speaker norms, highlighting the practical necessity for speakers to negotiate meanings across cultural divides. While Jenkins does not concentrate on security issues, her insights have informed numerous subsequent studies on how English can be leveraged – or, at times, misused – amid international crises and negotiations.

A growing number of scholars have begun connecting intercultural communication research directly to information security and the prevention of conflict escalation. For instance, Anakwah et al. in their article "The effect of authority on eyewitness memory reports across cultures" in *Psychiatry, Psychology and Law* argue (Anakwah, 2024) that cultural stereotypes and linguistic ambiguities are systematically exploited to spread disinformation. Their empirical analysis, carried out in regions of Eastern Europe (excluding Russia and Belarus), demonstrates how strategic actors capitalise on cultural fault lines to manipulate narratives – an issue alarmingly pertinent to Ukraine and its international partners.

In a similar vein, Darwin & Norton have expanded upon the notion of "investment" in multilingual settings, illustrating (Darvin, 2016) in *Langage et société* how digital platforms offer both opportunities and risks for learners who navigate online communities shaped by various cultural influences. Their study, while focusing primarily on education, has direct implications for understanding how individuals in Ukraine might participate in global dialogues about the war, discerning credible sources from propaganda, and

collaborating with international allies on humanitarian or conflict-resolution initiatives.

Additionally, Ting-Toomey have contributed a valuable piece entitled “Intercultural Conflict Training: Theory-Practice Approaches and Research Challenges.” published in *Journal of Intercultural Communication Research*. The authors examine (Ting-Toomey, 2017) real-life negotiation scenarios involving English as a common working language among parties from different cultural backgrounds. Though their data set spans several geographical regions, it encapsulates a variety of conflict contexts, offering parallels to Ukraine’s diplomatic efforts to secure support and articulate its stance to various international actors. Their findings suggest that intercultural competence significantly reduces misinterpretations and fosters greater trust, reinforcing the chapter’s argument that effective communication is an indispensable pillar of security.

Recognising the unique challenges posed by the Russian-Ukrainian war of aggression, a number of Ukrainian researchers have sought to adapt intercultural frameworks to the present realities of the country. Borysenko & Vysotska, for example, in “Media Literacy: Ukrainian Perspective”, highlight the urgent need for language curricula that develop students’ abilities to critically evaluate media sources. Their empirical work shows (Borysenko, 2018) that the deliberate misrepresentation of information across different media channels has magnified the potential for cultural misunderstandings. Such findings underscore the necessity of teaching intercultural communication not as an abstract ideal, but as a concrete skill set crucial for national security and global awareness.

Similarly, Konovalova investigates how multilingual practices among Ukrainian students can bolster cultural empathy. While her focus is primarily on everyday classroom discourse, the study’s conclusions regarding students’ capacity to engage productively with cross-cultural material dovetail with broader themes of how language use and cultural knowledge mitigate (Konovalova, 2024) the risk of conflict, both domestically and internationally.

Despite the progress outlined above, significant gaps in the literature remain. Firstly, the interplay between digital disinformation and intercultural communication requires more specialised empirical attention. Although Anakwah et. al. begin to address this issue, the rapidly evolving nature of social media platforms and emerging communication technologies calls for (Anakwah, 2024) ongoing investigation. Specifically, there is a dearth of longitudinal studies that track how new digital channels (e.g., AI-driven messaging apps, encrypted networks) shape user perceptions in war-affected zones such as Ukraine.

Secondly, the psychological impact of prolonged conflict on intercultural communication competences remains underexamined. While existing scholarship convincingly argues that intercultural skills foster empathy and trust, there is limited understanding of how sustained exposure to war, displacement, or trauma might alter individuals’ ability – or willingness – to engage openly across cultural boundaries. More integrative research is needed to link fields like psycholinguistics, conflict studies, and intercultural education to address this issue.

Finally, the complexity of implementing intercultural communication training in emergency contexts has yet to be thoroughly studied. Many programmes assume a stable environment in which learners can safely experiment with unfamiliar cultural perspectives. In conflict-affected regions, however, logistical disruptions, emotional distress, and immediate survival needs can overshadow efforts to promote intercultural dialogue.

Developing a flexible framework that can be adapted swiftly for crisis settings could profoundly benefit those grappling with the realities of war, as is the case in Ukraine.

Taken collectively, the works by Byram, Kramsch, Jenkins, Anakwah, Darwin, Norton, Ting-Toomey, Borysenko, Vysotska, Konovalova, and many others represent a solid foundation upon which further inquiry into intercultural communication and information security can be built. Their research clarifies how intercultural competence can mitigate misunderstanding, strengthen alliances, and address the spread of disinformation – particularly salient considerations as Ukraine confronts ongoing aggression. Yet crucial questions linger regarding the dynamic interplay between digital technologies, conflict psychology, and practical pedagogical strategies in volatile environments. Addressing these gaps will not only enrich academic discourse but also hold tangible implications for policy-makers, educators, and communities seeking to preserve security and foster genuine international cooperation.

2. Features of the linguistic and cultural context

The linguistic and cultural context of any conversation or document is crucial in shaping how information is conveyed and interpreted. When dealing with multilingual communication, the primary challenge emerges (*Nykyporets, 2024*) from differences in syntax, vocabulary, and idiomatic expressions. Words in one language may not have an exact equivalent in another, prompting translators to choose approximate terms or resort to clarifications that might still fall short of capturing the original meaning. In an international business negotiation, for instance, using a term that has a strong negative connotation in the other party's language could derail trust and goodwill, even if the speaker did not intend any offense.

Beyond the purely linguistic elements, cultural factors greatly influence the perception of information. Cultures vary in their understanding of personal space, hierarchy, symbolic gestures, and social norms, all of which can colour the interpretation of a message. A hand gesture that is friendly or neutral in one part of the world may be considered offensive in another. Even colour symbolism – such as the meaning of white, red, or black – differs widely from culture to culture. An image or logo employing certain colours could unintentionally convey the wrong message, thereby causing confusion or discomfort.

A notable illustration of these cultural and linguistic nuances is found in the translation of proverbs and idiomatic expressions. A phrase that is meant to be humorous in one culture could be perceived as inappropriate, confusing, or even insulting in another. For example, the English phrase “break a leg,” commonly used to wish someone good luck, literally translates into many languages as an ominous suggestion of causing physical harm. Without a deep understanding of the cultural context, the intended meaning of encouragement is lost entirely. Similarly, direct translations of terms like “deadline” or “long shot” might not carry the same urgency or metaphorical weight outside of English-speaking environments, potentially leading to serious misinterpretations in professional or diplomatic contexts.

Cultural stereotypes add another layer of complexity to intercultural communication. Preconceived notions about a particular group's behaviour, communication style, or values can bias how messages from that group are interpreted. For example, a team member from a culture stereotyped as “submissive” or “non-confrontational” might have their contributions undervalued or misunderstood in an international meeting. Such biases can

hamper effective collaboration, cause conflicts, and lead to decisions based on flawed assumptions rather than factual evidence.

3. Risks to information security

While misinterpretation can disrupt day-to-day communication and collaboration, it also poses significant risks to information security. In an era of rapid information exchange, a small misunderstanding can escalate and have far-reaching consequences. For instance, a misinterpretation of technical documentation or security protocols in a multinational company could result in incorrectly implemented safeguards, leaving critical systems vulnerable to cyber threats. When large-scale operations rely (Nykyporets, 2023) on precise instructions and timely coordination – such as in aviation, international finance, or cybersecurity – clarity of language and a shared understanding of terminology are paramount.

Misinterpretation also opens the door to manipulation and disinformation. Malicious actors, including hackers and propagandists, often exploit linguistic and cultural nuances to sow confusion or spread false narratives. A carefully crafted message that capitalizes on cultural biases or ambiguities can be particularly effective, as it targets existing blind spots in a multicultural audience. For example, disinformation campaigns may use culturally tailored messages to stir tensions or mistrust between different groups, ultimately undermining social cohesion or weakening the defences of international alliances.

The globalized flow of information amplifies these risks. In many cases, a single misinterpretation of an official statement or diplomatic document, once reported by international media, can influence the perceptions and reactions of millions of people. News agencies and social media platforms play a pivotal role in rapidly disseminating stories around the world, but they also become echo chambers where initial misunderstandings can be repeated, exaggerated, or deliberately twisted. Consequently, misinterpretation can escalate into full-blown crises, impacting international security and undermining efforts to maintain stable relations between nations.

Additionally, language barriers within international organizations or partnerships can hinder the effective coordination of security measures. For instance, cybersecurity experts in different countries might use standardized English terminology but interpret certain terms differently due to regional language influences. If a single term, like “firewall configuration,” carries slightly different operational meanings in various contexts, the resulting confusion may lead to inconsistent implementations, thereby compromising overall security.

4. Finding ways to overcome the risks

To mitigate the risks associated with misinterpretation in multicultural environments, a multifaceted strategy is required – one that acknowledges the importance of both linguistic accuracy and cultural sensitivity. Below are some approaches and resources that individuals, institutions, and governments can employ the following.

a) Attention to context. Encouraging communicators to provide detailed context can drastically reduce misinterpretation. Rather than assuming shared knowledge or cultural norms, individuals should offer background information, define specialized terms, and clarify any idiomatic language. This can be facilitated by internal guidelines or training programs that promote context-rich communication.

b) Clarification and feedback. Open channels of communication are essential.

Participants should be encouraged to ask questions, request rephrasing, or seek elaboration. Active listening skills, such as summarizing and paraphrasing, help confirm that the intended meaning has been understood. In a business setting, periodic feedback loops – both verbal and written – can prevent small misunderstandings from escalating into costly errors.

c) Fact-checking and verification. In an era of rapid information sharing, fact-checking and verification play a critical role in combating disinformation. Institutions should foster a culture of scepticism, where information is scrutinized and checked against credible sources. This is particularly important when dealing with multilingual content, as subtle translation errors can significantly alter facts. Cross-referencing information in different languages can also highlight potential discrepancies or manipulations.

d) Language and cultural training. Providing language and cultural training for professionals who engage in international or intercultural work can significantly decrease the risk of misinterpretation. This includes teaching not just vocabulary and grammar, but also pragmatic and sociocultural aspects of communication. Training programs that focus on cultural awareness – covering values, customs, and communication styles – help individuals understand how to adapt their language for diverse audiences.

e) Use of professional interpreters and translators. In high-stakes situations, relying on professional translators and interpreters with specialized knowledge of the relevant fields (e.g., legal, medical, technical) can prevent critical errors. These professionals are trained to capture nuances and context that automated or less-qualified translators might miss. Even so, it is crucial to provide them with sufficient background information and maintain a process of review to ensure accuracy.

f) Technological aids. Language technology, such as machine translation tools, can be useful in bridging language barriers quickly. However, these tools should be supplemented by human expertise to handle contextual and cultural nuances effectively. Furthermore, glossaries of key terms that are regularly updated can help ensure consistency in terminology across different departments or regions.

g) Inclusive communication policies. Organizations can implement policies that require important documents, memos, or announcements to be translated into multiple languages for multilingual audiences. Such practices demonstrate respect for cultural diversity and help diminish the potential for misinterpretation. Inclusivity in communication also fosters an environment where individuals feel comfortable expressing doubts or concerns, thereby further reducing risks.

In an era marked by extensive international cooperation and interdependence, the stakes for accurate and effective communication have never been higher. Misinterpretation in a multicultural environment is a multifaceted challenge that touches upon linguistic subtleties, cultural values, social norms, and cognitive biases. As this chapter demonstrates, these misunderstandings can have significant repercussions – not only in everyday interactions but also in the domain of information security, where misinterpretation may lead to large-scale vulnerabilities, the spread of disinformation, and ultimately the destabilization of global networks.

The strategies outlined above – such as contextualizing information, encouraging feedback, employing professional translators, and integrating cultural training into professional development – are practical steps toward mitigating the risks posed by misinterpretation. Nonetheless, no strategy can fully eliminate the possibility of

misunderstanding in a world as diverse and fast-changing as ours. What can be achieved, however, is a heightened awareness of the critical role that language and culture play in shaping communication outcomes.

By acknowledging that every message is interpreted through a prism of cultural and linguistic assumptions, communicators can become more vigilant and proactive in identifying potential sources of error. This attentiveness is crucial for safeguarding information security, strengthening international relations, and fostering a culture of mutual respect and understanding. As we proceed to the next chapter, we will delve deeper into how culture itself can be both a source of conflict and a cornerstone of conflict prevention. Through this exploration, we continue to build on the central theme that intercultural competence is not just an academic ideal, but an essential skill for thriving in an interconnected and often turbulent global arena.

II. Culture as a potential source of conflict or conflict prevention when it comes to security and information sharing

1. Introduction to the topic of culture and information security

As our world grows ever more connected, the role of culture in shaping security practices and information-sharing protocols cannot be overstated. Culture, broadly defined, refers to a system of values, norms, beliefs, and behavioural patterns that individuals inherit from the societies in which they live. This system – often deeply ingrained from an early age – profoundly influences how people interpret the world around them, make decisions, and interact with others. As a result, cultural factors significantly impact how different communities perceive threats, manage risks, and handle sensitive information.

When considering issues of security and information sharing, it is crucial to recognize that cultures vary in their approach to confidentiality, openness, and the balance of collective versus individual responsibility. For instance, in some societies, maintaining strict hierarchies and respecting authority are valued above all else, leading to a more centralized (Hyatt, 2023) and controlled approach to security measures. In others, a higher emphasis on individual rights and freedoms fosters a more decentralized system, where transparency and shared responsibility are prioritized. These divergences underscore the importance of cultural awareness: a policy or protocol that is highly effective in one setting might be met with resistance or confusion in another.

In practical terms, cultural differences manifest in everything from password-sharing habits among colleagues to the willingness of citizens to accept governmental surveillance. A culturally tuned perspective enables policymakers, security experts, and multinational organizations to develop strategies that are not only effective but also culturally sensitive, thus reducing friction and enhancing trust. Neglecting the cultural underpinnings of security (Fanjanirina, 2024) can lead to misalignment of objectives, increased misunderstandings, and ultimately, a higher risk of conflict. Conversely, recognizing these factors can foster a cooperative environment that promotes mutual understanding, facilitating both conflict prevention and effective collaboration.

2. Culture as a source of conflict

While culture can serve as a bridge to understanding, it can also become a source of tension and discord when communication, values, or expectations clash. One example lies in differing attitudes toward confidentiality: in some cultures, sharing information within an in-group (e.g., family, close friends, or trusted colleagues) is considered a natural extension

of relationships, while in others, strict boundaries define what can and cannot be disclosed, even within private circles. In international business collaborations, such contrasting norms can fuel disagreements, as one party may perceive information withholding as secrecy or mistrust, and the other might see casual sharing as a security breach.

Ethical and moral frameworks also vary substantially across cultures. Approaches to privacy, intellectual property, and the “right to know” often depend on deeply held societal values. For instance, in a society that prioritizes collective well-being, government surveillance might be accepted – If not outright encouraged – as a necessary trade-off for community safety. In a culture with a stronger focus on individual autonomy, the very same measures might be viewed as invasive overreach. Such conflicting viewpoints can create friction, especially in multinational negotiations or within international organizations attempting to standardize security protocols.

Another potential source of conflict arises from differing levels of directness or indirectness in communication. Some cultures prefer explicit directives and place a high value on clarity, which can lead to more transparent but sometimes rigid security approaches. Others rely on indirect cues or place emphasis on preserving harmony within a group, potentially resulting in ambiguous communication about sensitive matters. This indirect style can cause misunderstandings and mistrust if other parties interpret it as evasion or withholding crucial information. In this way, cultural communication styles may inadvertently escalate disagreements that could have been avoided with clearer mutual understanding.

Taken together, these examples demonstrate how misalignments in cultural expectations can lead to suspicion, frustration, and even overt conflict when dealing with issues of security and information sharing. Identifying these potential points of contention and acknowledging their cultural underpinnings are the first steps toward mitigating conflicts before they escalate.

3. Culture as a tool for conflict prevention

On the other hand, culture is not solely a harbinger of conflict. In fact, it can serve as a powerful tool for building bridges, facilitating dialogue, and preventing misunderstandings. When approached thoughtfully, cultural awareness can foster a climate of respect and cooperation, in which shared goals and common interests in security are emphasized (*Lam, 2021*) over existing differences.

One way culture contributes to conflict prevention is by promoting empathy and mutual understanding. When individuals understand that security protocols are shaped by deeply entrenched norms and values, they are more likely to view each other’s decisions in a sympathetic light – even if they do not personally agree with them. This recognition encourages constructive dialogue rather than defensive reactions. For example, an international task force working on counterterrorism might incorporate cultural studies into its training program, enabling each member to grasp the historical and societal factors that influence how another nation perceives and handles threats.

Methods of cultural adaptation, such as intercultural diplomacy and cultural sensitivity training, provide practical frameworks for bridging differences. Intercultural diplomacy involves tailored communication strategies that honour the other party’s cultural context, ensuring that security objectives are clearly understood. This approach can be especially beneficial in negotiations over sensitive topics like data sharing or arms control, as parties feel

respected and validated in their cultural standpoint, reducing the chance of an impasse.

Cultural sensitivity training, on the other hand, equips individuals in multinational corporations, non-governmental organizations, and government agencies with the knowledge to navigate cross-cultural interactions effectively. By learning about various communication styles, decision-making processes, and even conflict-resolution techniques, professionals can proactively address potential misalignments. This pre-emptive strategy goes a long way in diffusing tension before it has the chance to escalate into a full-blown crisis.

Ultimately, fostering a sense of cultural competence within international organizations can help maintain stability and security. Cultural competence implies that an organization and its members are not merely tolerant of diversity but are actively seeking to understand and integrate various cultural perspectives in their protocols and strategies. This holistic approach strengthens internal cohesion, engenders trust among international partners, and lays the groundwork for effective collaboration on security issues.

4. The role of intercultural communication in conflict prevention

Intercultural communication skills are foundational to both recognizing the triggers of conflict and deploying effective prevention strategies. Training programs that offer exposure to different cultures – through language studies, cultural immersion, or experiential learning – equip individuals with the empathy and adaptability needed to navigate complex situations where misinformation or suspicion could quickly spiral into dispute.

In many global organizations, structured intercultural programs involve not only language training but also (*Nykyporets, 2024*) practical exercises in negotiation, problem-solving, and conflict resolution. By simulating real-world scenarios, participants gain firsthand insight into how cultural nuances can reshape the dynamics of a conversation or negotiation. This experiential approach reveals potential pitfalls in information sharing, helping future leaders and decision-makers become vigilant about tailoring their communication to diverse audiences.

Trust-building is another critical component of intercultural communication. Trust does not emerge spontaneously in multicultural contexts; it must be carefully cultivated and reinforced through transparent communication, consistent behaviour, and a willingness to listen. Developing trust is especially pivotal in the realm of security, as parties must rely on each other to follow through with agreements, respect confidentiality, and share accurate information. Intercultural communication training that emphasizes trust-building strategies – such as demonstrating respect for alternative viewpoints, practicing active listening, and offering clarity where ambiguity may arise – can significantly mitigate the risk of conflict.

Ultimately, well-implemented intercultural communication programs contribute to greater stability and cooperation in international relations. By equipping stakeholders – from diplomats to intelligence analysts – to communicate effectively (*Fedorenko, 2024*) across cultural divides, these programs reduce the likelihood that minor misunderstandings will escalate into major disputes. In this way, intercultural communication serves as a proactive line of defence against conflict in security and information-sharing environments.

Culture wields a profound influence on how nations, organizations, and individuals approach both security and information sharing. As this chapter has shown, culture can function as a potential source of conflict when contrasting values, norms, and communication styles are not fully understood or respected. However, the same cultural considerations, when leveraged effectively, serve as a powerful tool (*Medvedieva, 2023*) for

conflict prevention. By recognizing where cultural flashpoints may lie and actively working to foster intercultural understanding, stakeholders in global security contexts can create more stable and cooperative environments.

Indeed, those who appreciate the cultural dimension of security and information sharing are in a better position to design protocols and strategies that account for diverse perspectives. This approach (*Croucher, 2012*) not only helps avert misunderstandings that could jeopardize trust and safety but also ensures that varied viewpoints are included, often leading to more robust and equitable solutions. As we look ahead to the next section – dedicated to teaching intercultural communication within professional and educational curricula – we will delve deeper into how organizations and institutions can cultivate these competencies on a systematic level. Through structured training programs and policy reforms, it is possible to elevate cultural awareness from a theoretical ideal to a practical skill set that meaningfully contributes to international security and cooperation.

III. Implementing intercultural communication in English language curricula

1. The importance of intercultural communication in the curriculum

In the twenty-first century, English language education extends well beyond the mere acquisition of grammar and vocabulary. As globalisation accelerates, learners of English increasingly encounter situations in which they must engage with diverse perspectives, negotiate meaning across cultural boundaries, and navigate international contexts. These realities highlight the critical importance of intercultural communication – the ability to interact effectively and appropriately with people from different cultural backgrounds – within English language curricula.

From a theoretical standpoint, intercultural communication may be defined as the intersection of linguistic competence, cultural awareness, and empathetic engagement with others. In practical terms, it involves skills such as recognising cultural nuances in tone and body language, adapting communication styles to different social norms, and demonstrating respect for values and behaviours that may differ from one's own. Within the classroom, placing intercultural communication at the heart of English language teaching helps learners develop a more holistic grasp of the language. Not only do they learn how to construct accurate sentences, but they also acquire the socio-pragmatic awareness needed to interpret and respond to communicative cues in authentic settings.

Cultivating intercultural competences in English lessons (*Nikolaeva, 2017*) is especially pertinent in the Ukrainian context, where recent geopolitical and social upheavals – most notably, the Russian-Ukrainian war of aggression – have underscored the necessity of forging international alliances and promoting global understanding. As the conflict has drawn worldwide attention, Ukraine's engagement with international organisations, humanitarian agencies, and foreign partners has intensified. English, serving as the *lingua franca*, stands (*Bingzhuan, 2021*) at the epicentre of these endeavours, functioning not merely as a tool for information exchange but also as a platform for fostering empathy, solidarity, and mutual support.

Indeed, the reality of war has illuminated the extent to which effective communication can influence decision-making processes and crisis management efforts on the global stage. Students – whether they aspire to careers in diplomacy, business, international relief work, or academia – require strong intercultural competences to operate efficiently in multinational environments. Embedding intercultural communication into the English

language curriculum thus enhances learners' adaptability, preparing them to cope with unfamiliar cultural norms and swiftly changing international conditions.

2. Integrating intercultural communication into the English language programme

Modern approaches to teaching intercultural communication within English courses span a broad spectrum, from explicit curriculum design to more implicit, learner-centred methods. In recent years, language educators have increasingly recognised the value of combining linguistic content with cultural insights, thus fostering (Nykycorets, 2023) both communicative accuracy and intercultural awareness. The following are several strategies for weaving these dimensions into English language programmes:

a) **materials from diverse cultures.** Rather than relying solely on textbooks that reflect a single cultural perspective, educators can incorporate authentic resources – such as articles, short stories, films, and podcasts – from a variety of English-speaking communities worldwide. This practice not only broadens students' cultural horizons but also prompts them to compare and contrast values, historical contexts, and linguistic expressions across regions.

b) **real-life situations of international communication.** Role-plays, simulations, and project-based activities can closely replicate global interactions. For instance, students might engage in a mock United Nations debate on international security issues, drawing parallels to the experiences of Ukraine's appeals for defensive support and humanitarian assistance. By adopting diverse viewpoints, learners gain an appreciation for the cultural, political, and emotional factors that shape international dialogues.

c) **exploration of cultural aspects through role-playing and discussions.** Interactive exercises that invite learners to take on the perspectives of people from other cultures facilitate both linguistic practice and empathy-building. Consider scenarios where students must negotiate bilateral agreements or discuss relief efforts, referencing real-world events such as the ongoing Russian-Ukrainian war. Discussions that tackle ethical concerns – like civilian protection or media integrity – can also enhance learners' critical engagement with global challenges.

d) **inclusion of topics related to global issues.** Incorporating pressing global topics – such as climate change, human rights, technological advancements, and international security – helps students connect their language-learning experience with contemporary world affairs. In Ukraine, the war has heightened public consciousness around issues of sovereignty, freedom of information, and cybersecurity. By featuring these themes in class discussions or reading assignments, educators can (Nykycorets, 2024) nurture critical thinking and global-mindedness, vital traits in both academic and professional contexts.

By systematically integrating intercultural components into English programmes, educators across Ukraine – and indeed elsewhere – pave the way for a generation that is linguistically proficient and globally engaged. In light of the war's devastating humanitarian impacts and the rapid international response, there has never been a more pertinent time to equip learners with the skills to communicate and collaborate on a worldwide stage.

3. Developing critical thinking and tolerance through intercultural communication

Embedding intercultural communication within English language teaching not only enriches learners' linguistic abilities but also fosters critical thinking and tolerance – two

attributes of paramount importance in any pluralistic society. Critical thinking involves the capacity to analyse information, question assumptions, and evaluate evidence from multiple angles before reaching conclusions. Tolerance, closely linked to empathy and open-mindedness, allows individuals to respect and value cultural differences without resorting to prejudice or hostility.

Contribution to critical thinking

When students are confronted with intercultural scenarios, they are required to look beyond their immediate worldview and consider alternative viewpoints. Engaging with texts or media depicting conflicts, negotiations, or misunderstandings rooted in cultural differences obliges learners to unpack the complexities of each scenario. For example, discussing how Western and Eastern European media outlets depict the Russian invasion of Ukraine differently can challenge learners to assess bias, verify sources, and recognise the broader socio-political underpinnings of war coverage. Such exercises cultivate analytical skills that extend (*Nykyporets, 2024*) far beyond language learning, shaping informed global citizens who can navigate the complexities of international relations.

Building tolerance

The war in Ukraine has underscored the destructive potential of unchecked intolerance and aggression, making it increasingly clear that a globalised world requires a profound commitment to mutual respect and understanding. Classroom activities that centre on intercultural communication – whether via group projects, debates, or cross-border pen-pal exchanges – offer a microcosm in which learners practise tolerance and empathy. A teacher's role here is invaluable; by moderating discussions, encouraging the respectful exchange of opinions, and guiding students towards constructive solutions, educators model the attitudes and behaviours needed to overcome misunderstanding.

In offering structured opportunities for learners to explore cultural conflicts and cooperative resolutions, English language classes become a laboratory for honing these crucial social and cognitive competences. This dual emphasis on critical thinking and tolerance ensures that students graduate with the disposition to question narratives, challenge stereotypes, and engage peacefully in diverse settings.

4. Methodological strategies and tools for English language teachers

The successful integration of intercultural communication into English language programmes depends on both methodological innovation and practical resources. Teachers who embrace creative strategies, modern technologies, and collaborative projects can significantly enhance their students' ability to operate in cross-cultural contexts.

a) Online resources and multimedia materials.

The proliferation of web-based learning platforms, virtual libraries, and media archives has made it increasingly feasible for teachers to introduce global content into the classroom. Ukrainian educators, for instance, can access open-access repositories of documentary films or news segments covering aspects of the war, which can then serve as a catalyst for discussions on perspective-taking and ethical reporting. Interactive tools (e.g., Padlet, Flipgrid, Kahoot) allow learners to share reflections, create (*Nykyporets, 2023*) multimedia projects, and collaborate with peers in real time, thereby reinforcing the link between language learning and intercultural awareness.

b) Global platforms for intercultural communication.

Video conferencing services and social media platforms can connect Ukrainian

students with peers in other countries – whether for language exchange programmes or joint class projects. Such interactions offer direct exposure to alternative viewpoints, bridging the gap between abstract concepts of “culture” and real-life human experiences. By discussing everyday topics (e.g., family traditions, societal norms, current affairs) in English, learners hone both their linguistic skills and their capacity to empathise with others.

c) Intercultural projects and partnerships.

Establishing partnerships with schools, universities, or non-profit organisations abroad fosters authentic intercultural engagement. Projects focusing on themes like humanitarian relief, refugee support, or environmental sustainability can particularly resonate in war-affected regions of Ukraine, as students witness tangible examples of collective problem-solving. These initiatives also encourage participants to consider cultural sensitivities when setting objectives, dividing tasks, or interpreting results – an invaluable lesson in leadership and cooperation.

Examples of successful cases

A growing body of case studies demonstrates how purposeful inclusion of intercultural communication yields improved learner outcomes. Some Ukrainian secondary schools, for example, have implemented “*Global Perspectives*” modules (<https://surl.li/wccuyf>) within their English curriculum, drawing parallels between local challenges – such as rebuilding conflict-affected infrastructure – and broader global concerns like post-war reconciliation. Student feedback from these programmes frequently highlights enhanced motivation to learn English, greater confidence in international communication, and a deeper sense of global citizenship.

Example 1. English for resilience (British Council in Ukraine)

One notable success has been the British Council’s “English for Resilience” (<https://surl.li/mpxqiz>) initiative, which aims to provide comprehensive language and intercultural training for internally displaced persons and refugees in Ukraine. By offering not only language lessons but also intercultural workshops, the programme helps (Fedoriv, 2023) participants understand diverse social norms and communication styles, particularly relevant when seeking international support or relocating to host countries. Feedback from participants suggests (Kharchenko, 2019) they not only improved their English proficiency but also learned to better navigate global contexts – building empathy and dispelling cultural myths that might otherwise hinder effective cooperation. By involving local communities, schools, and non-governmental organisations, the programme successfully bridges cultural gaps and fosters a sense of solidarity among diverse social groups affected by the war.

Based on the British Council’s “English for Resilience” initiative, here are some practical recommendations for Ukraine during the ongoing war. These recommendations draw directly from the principles demonstrated in the British Council’s “*English for Resilience*” initiative, emphasizing language as a bridge for understanding, adaptation, and personal growth in challenging circumstances.

Table 1.

Practical recommendations for Ukraine during the ongoing war.

	Task	Description	Practical advice
1.	Prioritize language and cultural	The “English for Resilience” program highlights the	1. Develop comprehensive language support programs that go beyond basic language instruction. 2. Create intercultural workshops that help refugees and

	adaptation	critical importance of language skills and cultural understanding for displaced individuals.	displaced persons understand communication norms in potential host countries. 3. Provide targeted language training that focuses on practical skills needed for job seeking, education, and social integration.
2.	Build psychological resilience through communication	Language learning can be a powerful tool for psychological support	1. Design language programs that incorporate emotional intelligence and communication skills. 2. Use language classes as safe spaces for participants to share experiences and build support networks. 3. Integrate storytelling and personal narrative techniques to help individuals process trauma and build confidence.
3.	Leverage technology for accessible learning	Given the challenges of war-time displacement	1. Develop mobile and online language learning platforms 2. Create downloadable resources that can be accessed with limited internet connectivity 3. Develop offline learning materials for areas with restricted technological access
4.	Community-cantered approach	Following the initiative's successful model	1. Involve local communities, schools, and NGOs in language and integration programs. 2. Create peer-support networks for language learners. 3. Develop mentorship programs connecting displaced individuals with local and international support networks.
5.	Skill-specific language training	Tailor language programs to practical needs	Create specialized English courses for: a) job market integration b) academic preparation c) healthcare communication d) navigating bureaucratic systems in potential host countries
6.	Psychological and cultural support integration	Holistic support addressing mental health and cultural adaptation challenges.	1. Provide counselling resources alongside language training. 2. Offer workshops on cultural adaptation and stress management. 3. Create safe spaces for discussing challenges of displacement and cultural transitions.
7.	International collaboration	Global knowledge exchange and shared learning across international boundaries.	1. Seek partnerships with international language institutions. 2. Develop exchange programs and collaborative learning platforms. 3. Create scholarships and support for continued education abroad.

Source: Created by authors.

The key is to view language learning not just as a technical skill, but as a holistic tool for personal empowerment, psychological resilience, and social integration during challenging times of displacement and conflict.

Example 2. Cultural Bridges (EU-Ukraine Collaborative Project)

“Cultural Bridges,” (<https://surl.li/iylzbe>) co-funded by the European Union, stands out for its systematic approach to promoting intercultural dialogue and mutual understanding in conflict-affected regions of Ukraine.

Below is a table offering practical recommendations for Ukraine during the ongoing

war, drawing on the strategies and outcomes observed in the “Cultural Bridges” programme. These recommendations can be adapted to various regional contexts, reflecting local linguistic and cultural nuances.

Table 2.

Practical recommendations for Ukraine

	Tasks	Description	Practical Advice
1.	Expand cultural programmes	Increase the scope and diversity of workshops, joint artistic performances, and multilingual publications to foster cross-cultural dialogue and shared values across communities – particularly in conflict-affected areas.	Collaborate with local community centres, NGOs, and international donors to secure resources for additional events. Encourage participants from different backgrounds and age groups to ensure inclusivity.
2.	Facilitate safe spaces for expression	Provide venues – whether physical or virtual – where citizens can safely articulate their experiences of aggression and loss, enabling them to process trauma and build narratives that resonate with global audiences.	Partner with mental health professionals and experts on conflict resolution to create trauma-informed sessions. Ensure security protocols for gatherings, especially in regions with ongoing hostilities.
3.	Strengthen community engagement and ownership	Encourage active involvement of local educators, artists, and media representatives in planning and executing intercultural events, thus deepening the sense of community ownership and responsibility for peaceful coexistence.	Develop local advisory committees or task forces that represent multiple stakeholder groups. Offer leadership and project-management training for community members to sustain initiatives autonomously.
4.	Promote cross-border collaboration and visibility	Connect with international cultural and educational institutions to exchange strategies, showcase success stories, and attract global attention to the resilience and creativity of Ukrainian communities under threat.	Seek partnerships with foreign universities, cultural organisations, and art collectives. Capitalise on digital platforms – social media, virtual exhibitions, live-streamed performances – to reach a wider audience.
5.	Integrate conflict resolution skills into cultural activities	Weave conflict resolution techniques, such as mediation and dialogue facilitation, into all programme activities to address tension points constructively and prevent misunderstandings from escalating.	Train facilitators in intercultural communication and peacebuilding methodologies. Encourage reflective discussions after each event to assess and improve collaborative problem-solving efforts.

Source: created by authors.

Targeting educational institutions, cultural centres, and media outlets, the project facilitates workshops, joint artistic performances, and multilingual publications that emphasise shared values rather than differences. This platform has proven particularly effective in helping communities articulate their experiences of aggression and loss in ways that resonate with international audiences. Participants report heightened awareness of cultural commonalities, reduced (*TIALT, 2024*) reliance on stereotypes, and improved skills in conflict resolution – especially crucial in areas where tensions may remain high. As a result, “Cultural Bridges” has garnered international recognition as a replicable model for

fostering coexistence and resilience amid challenging geopolitical circumstances.

In alignment with “Cultural Bridges,” collaboration among educational institutions, cultural centres, and media outlets remains vital for creating a broader impact and fostering enduring resilience.

Example 3. Intercultural partnerships at Ukrainian universities

A third example of successful intercultural engagement comes from Taras Shevchenko National University in Kyiv and National Technical University in Vinnytsia. Taras Shevchenko National University has established partnerships with universities across Europe, North America, and Asia to develop shared English-language modules. These modules incorporate thematic units on international relations, crisis management, and cultural awareness, all taught by a team of multilingual lecturers with diverse cultural backgrounds. Students not only refine their language skills but also engage in cross-border projects – such as virtual debates, peer reviews of research papers, and co-authored digital presentations – where they practise negotiation, empathy, and consensus-building. Initial assessments suggest that participants gain a deeper understanding of how cultural assumptions can shape perceptions, a skill set indispensable for representing Ukraine’s interests in diplomatic, academic, or humanitarian contexts. By blending English instruction with global-minded curricula, Taras Shevchenko National University’s initiative stands as a testament to how higher education institutions can serve as incubators for intercultural competence and conflict prevention.

Vinnytsia National Technical University (VNTU) has entered into a partnership with the international IT company GlobalLogic to enhance the quality of IT education. This collaboration aims to provide VNTU’s 4,250 technical students with practical skills and insights into the IT profession, thereby improving (*GlobalLogic, 2024*) their readiness for commercial projects. The partnership includes modernizing curricula to align with current industry standards, offering students relevant practical experiences during their studies. This initiative is part of GlobalLogic’s broader educational program, which collaborates with 22 higher education institutions across seven Ukrainian cities.

Vinnytsia National Technical University’s partnership with GlobalLogic is a significant development in fostering intercultural and educational collaboration between academia and the global IT industry. This initiative emphasizes the integration of modern technological expertise into the university’s academic framework, ensuring that students gain practical, hands-on experience while still pursuing their studies.

Key aspects of the collaboration include the following.

1. Curriculum modernization. The partnership focuses on updating educational programs to reflect the current demands of the IT industry, bridging the gap between theoretical knowledge and practical application.

2. Skill development. Through joint efforts, the university aims to equip students with the skills required for real-world IT projects, enhancing their employability in global markets.

3. Global exposure. As part of the cooperation, students gain access to international standards and practices, providing them with a competitive edge and familiarity with cross-cultural IT environments.

4. Broad engagement. The partnership is part of GlobalLogic’s extensive educational initiative, which collaborates with multiple universities across Ukraine, highlighting a

commitment to fostering IT talent on a national and international scale.

5. Strengthening university-industry ties. This collaboration serves as a model for university partnerships with global corporations, emphasizing the importance of academia-industry linkages in preparing students for global opportunities.

Such partnerships position VNTU as a hub for producing highly skilled graduates capable of contributing to intercultural IT projects and advancing Ukraine's reputation as a centre for technological innovation and collaboration.

In a world constantly reshaped by political upheavals, shifting alliances, and emerging transnational threats, the role of intercultural communication in English language education grows ever more critical. As demonstrated in this chapter, embedding intercultural competencies within curricula transforms language learning into a transformative process, one that cultivates critical thinking, tolerance, and a capacity to interact effectively in multicultural settings. This transformation is particularly significant in the context of modern Ukraine, where the challenges of war necessitate robust international collaboration and the ability to communicate persuasively on the global stage.

By integrating a wide array of cultural resources, authentic global issues, and interactive technologies, educators can shape students into well-rounded communicators and informed citizens. In doing so, English language programmes cease to be mere academic exercises and become powerful means of preparing learners to engage constructively with today's interconnected world. The sections of this monograph provide a general conclusion and detailed recommendations for refining these curricular strategies, ensuring that intercultural communication remains a foundational element in the ongoing evolution of English language education.

Building upon this foundation, the continued evolution of English language education must prioritize the development of nuanced intercultural understanding. This means going beyond superficial acknowledgements of cultural differences and delving into the deeper complexities of diverse perspectives, values, and belief systems. It necessitates fostering empathy, not just tolerance, and encouraging learners to challenge their own preconceived notions about other cultures. Furthermore, the incorporation of intercultural communication should not be treated as an isolated module, but rather interwoven throughout the entire curriculum, across all levels and subject areas.

This holistic approach ensures that students are consistently exposed to diverse viewpoints and have ample opportunities to practice their intercultural communication skills in various contexts. The incorporation of real-world case studies, simulations, and role-playing activities can effectively bridge the gap between theory and practice, allowing students to experience the challenges and rewards of navigating intercultural interactions firsthand. The use of technology, such as virtual exchange programs and online collaborative projects, can further enhance this experiential learning, connecting students with peers from different cultural backgrounds and fostering a sense of global citizenship.

Moreover, educators themselves must be equipped with the necessary intercultural competence to effectively guide their students. Professional development programs focusing on intercultural communication strategies, cross-cultural psychology, and global awareness are crucial for empowering teachers to become facilitators of intercultural dialogue. The ongoing assessment of intercultural competence, both for students and educators, is also essential to ensure the effectiveness of these initiatives. This assessment should go beyond

simple knowledge recall and focus on evaluating students' ability to apply intercultural understanding in practical situations.

Ultimately, the goal is to cultivate "intercultural speakers" – individuals who are not only proficient in English but also possess the cultural intelligence and sensitivity to navigate complex, multicultural environments with confidence and respect. This requires a commitment to continuous improvement and adaptation, reflecting the dynamic nature of global interactions. By embracing this comprehensive approach, English language education can truly become a vehicle for promoting understanding, cooperation, and peace in an increasingly interconnected, and often turbulent, world. The benefits extend far beyond the classroom, shaping individuals who are prepared to contribute meaningfully to a global society characterized by diversity and interdependence. Future development of educational materials must emphasize adaptability and current events to ensure continued growth.

Consequently, the integration of current, real-world events is paramount to maintaining relevance and engagement within intercultural communication training. This necessitates a flexible curriculum that can adapt to emerging global issues and evolving geopolitical landscapes. Educators should actively incorporate news articles, documentaries, and authentic online resources to provide students with up-to-date perspectives on intercultural dynamics. Furthermore, encouraging critical analysis of media representations of different cultures is crucial in combating stereotypes and fostering nuanced understanding. The cultivation of digital literacy skills becomes integral, empowering students to navigate the complexities of online intercultural interactions. Facilitating discussions around contemporary challenges, such as global migration, climate change, and international conflicts, helps students connect their learning to tangible realities.

This approach fosters a sense of global responsibility and encourages proactive engagement in finding solutions to shared problems. By actively reflecting on these pressing issues, students develop a deeper appreciation for the vital role of effective communication in building bridges across cultures. The enduring aim is to cultivate ethically aware global citizens. Therefore, prioritizing these pedagogical strategies is not merely an educational enhancement, but a societal imperative.

Summary. In this chapter, we explored the complicated relationship between intercultural communication, information security, and education, placing these issues in the broader context of globalisation and, more specifically, the realities confronting modern Ukraine. The Russian-Ukrainian war of aggression has underscored the crucial role that effective, culturally sensitive communication plays in both domestic and international arenas. By examining the challenges posed by misinterpretation, the dual nature of culture as a potential source of conflict or a catalyst for conflict prevention, and the pedagogical strategies for embedding intercultural communication in English language curricula, we arrive at a comprehensive understanding of the urgent need to prioritise these matters in academic and professional spheres.

In the first part of this chapter, we discussed how misinterpretation of information in a multicultural environment can lead to serious consequences for both information sharing and security. By highlighting examples of linguistic and cultural nuances, we demonstrated that misunderstandings often arise not merely from language barriers but also from deeply entrenched values and norms. These misinterpretations can be particularly damaging in high-stakes situations – such as international policy-making, relief efforts, or wartime

communications – where clarity and shared understanding are vital. Drawing parallels with the current war in Ukraine, we noted how the rapid global circulation of information makes the dangers of misinterpretation all the more pronounced, potentially influencing public opinion and international responses to crises.

The second part delved deeper into culture as both a source of potential conflict and a mechanism for conflict prevention. Here, we emphasised that while cultural differences can exacerbate tensions – especially when values such as privacy, openness, or collective responsibility are at odds – they also serve as a powerful avenue for fostering mutual respect and understanding. By engaging in dialogue that recognises each side’s cultural foundations, conflicting parties can often uncover shared aspirations, facilitating more peaceful resolutions. This discussion is particularly relevant to Ukraine’s current context, where the international community’s varying attitudes toward sovereignty, democracy, and security have profound implications for global and regional stability. Recognising culture’s dual role is a crucial step in designing strategies that promote security, cooperation, and peaceful coexistence.

Finally, in the third part, we turned our attention to practical solutions – namely, how English language teachers might integrate intercultural communication into their curricula. We noted that modern approaches to language education must go beyond grammar and vocabulary, striving instead to equip learners with critical competences that enable them to interact confidently and respectfully in multicultural settings. Through the incorporation of materials representing diverse cultures, real-world simulations, and discussions on pressing international issues, teachers can help learners appreciate different perspectives and adapt their communication styles accordingly. This approach is exceptionally pertinent in Ukraine, where ongoing wartime conditions necessitate both robust engagement with international partners and a nuanced understanding of foreign perspectives. By fostering empathy, critical thinking, and cultural sensitivity, educators can develop a generation of students prepared to navigate – and positively influence – the global stage.

Taken together, this step-by-step plan – investigating the roots of intercultural misinterpretation, recognising culture’s capacity for conflict and conflict prevention, and applying these lessons within English language education – provides a clear framework for understanding why intercultural communication is so vital for information security and broader societal resilience. In a period marked by geopolitical turmoil, particularly in Ukraine, leveraging this knowledge is not simply an academic endeavour but an urgent priority. Whether in diplomatic negotiations, humanitarian coordination, or everyday cultural exchange, effective communication grounded in mutual respect and understanding can offer tangible benefits for peace, cooperation, and the safeguarding of essential information.

References:

- Paxton A., Roche J. M., Ibarra A., Tanenhaus M. K. Predictions of Miscommunication in Verbal Communication During Collaborative Joint Action. *Journal of Speech, Language, and Hearing Research*. 2021. Vol. 64, No. 2. P. 613–627. DOI: https://doi.org/10.1044/2020_JSLHR-20-00137.
- Byram M. Teaching and Assessing Intercultural Communicative Competence: Revisited. *Multilingual Matters*, 2020. DOI: <https://doi.org/10.21832/9781800410251>.
- Kramsch C. In Language as Symbolic Power. *Cambridge: Cambridge University Press*, 2020. DOI: <https://doi.org/10.1017/9781108869386>.

- Jenkins J., Morán Panero S. Global Englishes: A Resource Book for Students. 4th ed. *Routledge*, 2024. DOI: <https://doi.org/10.4324/9781003027805>.
- Anakwah N., Horselenberg R., Hope L., Amankwah-Poku M., van Koppen P. J. The effect of authority on eyewitness memory reports across cultures. *Psychiatry, Psychology and Law*. 2024. P. 1-15. DOI: <https://doi.org/10.1080/13218719.2024.2362133>.
- Darvin R., Norton B. Investment and Language Learning in the 21st Century. *Langage et société*. 2016. № 157. P. 19-38. DOI: <https://doi.org/10.3917/ls.157.0019>.
- Ting-Toomey S. Intercultural Conflict Training: Theory-Practice Approaches and Research Challenges. *Journal of Intercultural Communication Research*. 2007. Vol. 36, No. 3. P. 255-271. DOI: <https://doi.org/10.1080/17475750701737199>.
- Borysenko O. A., Vysotska S. S. Media Literacy: Ukrainian Perspective. *Science and Education a New Dimension. Pedagogy and Psychology*. 2018. Vol. VI (64), Issue 154. DOI: <https://doi.org/10.31174/SEND-PP2018-154VI64-03>.
- Konovalova N. Experience of bilingual countries in the issue of mastering the minority language: effective borrowing into preschool pedagogy of Ukraine in order to form foreign language communicative competence in children of middle preschool age. *ScienceRise: Pedagogical Education*. 2024. No. 1 (58). P. 46–55. DOI: <https://doi.org/10.15587/2519-4984.2024.298785>.
- Nykyporets S. S., Stepanova I. S., Hadaichuk N. M., Derun V. H., Medvedieva S. O. Evolving expressions: contemporary trends in English phraseology and their sociocultural implications. *Bulletin of Science and Education. Series «Philology»*. 2024. № 2(20). Pp. 19-33. DOI: [https://doi.org/10.52058/2786-6165-2024-2\(20\)-19-33](https://doi.org/10.52058/2786-6165-2024-2(20)-19-33).
- Nykyporets S. S., Herasymenko N. V., Chopliak V. V. Cognitive strategies impacting the structural composition of translated technical and scientific texts: an analysis of translation methodologies. *Topical issues of translation of specialized texts: Scientific monograph*. Riga, Latvia : Baltija Publishing, 2023. P. 130-154. DOI: <https://doi.org/10.30525/978-9934-26-394-1-7>.
- Nykyporets S. S., Stepanova I. S., Ibrahimova L. V., Boiko Y. V., Chopliak V. V. Structural and semantic challenges of translating English terminological phrases within the specialized realms of energy and electrical engineering. *Bulletin of Science and Education. Series «Philology»*. 2023. № 12(18). Pp. 27-41. DOI: [https://doi.org/10.52058/2786-6165-2023-12\(18\)-27-41](https://doi.org/10.52058/2786-6165-2023-12(18)-27-41).
- Hyatt J., Gruenglas J. Ethical Considerations in Organizational Conflict. *IntechOpen*. 2023. DOI: <https://doi.org/10.5772/intechopen.1002645>.
- Fanjanirina J. The Effect of Cultural Differences on the Implementation of the African Continental Free Trade Area. *Open Journal of Business and Management*. 2024. Vol. 12. P. 51-78. DOI: <https://doi.org/10.4236/ojbm.2024.121005>.
- Lam L., Nguyen P., Le N., Tran K. The relation among organizational culture, knowledge management, and innovation capability: Its implication for open innovation. *Journal of Open Innovation: Technology, Market, and Complexity*. 2021. Vol. 7, No. 1. Art. 66. DOI: <https://doi.org/10.3390/joitmc7010066>.
- Nykyporets S. S., Boiko Yu. V. Practical tips and interactive learning tools for the work of a foreign language teacher at a technical university in the conditions of blended learning during the full-scale military aggression of Russia against Ukraine. *World trends in the use of interactive technologies in education. International collective monograph*. Intellebence Transportation System And Smart City Institute (ITSSCI). Lima, Peru, 2024. Chap. 14. P. 322-348. <https://doi.org/10.5281/zenodo.10653715>.
- Fedorenko Y., Martirosyan L. Intercultural communication as a key aspect of the modern world. *Актуальні питання гуманітарних наук*. 2024. Вип. 76, т. 3. С. 136-141. DOI: <https://doi.org/10.24919/2308-4863/76-3-23>.
- Medvedieva S. O., Stepanova I. S., Nykyporets S. S., Ibrahimova L. V. The application of a neuropsychological approach while teaching English to students of higher educational establishments. *Prospects and innovations of science. Series 'Pedagogy'*. 2023. № 8(26). С. 13-24. [https://doi.org/10.52058/2786-4952-2023-8\(26\)-13-24](https://doi.org/10.52058/2786-4952-2023-8(26)-13-24).
- Croucher S. M., Bruno A., McGrath P., Adams C., McGahan C., Suits A., Huckins A. Conflict Styles and High-Low Context Cultures: A Cross-Cultural Extension. *Communication Research Reports*. 2012.

- Vol. 29, No. 1. P. 64–73. DOI: <https://doi.org/10.1080/08824096.2011.640093>.
- Nykyporets S. S. The impact of modern information technologies on the training of technical translation. *International scientific and practical conference «Challenges of philological sciences, intercultural communication and translation studies in Ukraine and EU countries»* : conference proceedings, October 30–31, 2020. Venice : Izdevnieciba «Baltija Publishing», 2020. 337 pages. pp. 224–227. DOI: <https://doi.org/10.30525/978-9934-588-90-7-61>.
- Nikolaeva S. Intercultural foreign language education in Ukraine in the context of the secondary school reform. *Advanced Education*. 2017. Issue 8. P. 54–58. DOI: <https://doi.org/10.20535/2410-8286.111933>.
- Bingzhuan P. Intercultural communicative competence teaching and assessment based on modern information technology. *International journal of emerging technologies in learning (IJET)*. 2021. Vol. 16, no. 07. P. 175. DOI: <https://doi.org/10.3991/ijet.v16i07.21369>.
- Nykyporets S. S., Kot S. O., Boiko Yu. V., Melnyk M. B., Chopliak V. V. Advanced integration of virtual information environments (VIEs) in contemporary educational methodologies. *Society and national interests. Series «Education/Pedagogy»*. 2024. No. 4(4). Pp. 139–154. [https://doi.org/10.52058/3041-1572-2024-4\(4\)-139-154](https://doi.org/10.52058/3041-1572-2024-4(4)-139-154).
- Nykyporets S., Stepanova I., Nedobytko K. Advantages of using the project method in foreign language lessons as an effective method of teaching English to students of non-linguistic universities. *Norwegian Journal of Development of the International Science*. 2023. № 105. C. 53–57. DOI: <https://doi.org/10.5281/zenodo.7778961>.
- Nykyporets S. S., Melnyk O. D., Ibrahimova L. V., Hadaichuk N. M., Derun V. H. Advancing critical thinking skills among higher education students through English language instruction: contemporary approaches and strategies. *Prospects and innovations of science. Series «Pedagogy»*. 2024. № 1(35). Pp. 34–45. DOI: [https://doi.org/10.52058/2786-4952-2024-1\(35\)-34-45](https://doi.org/10.52058/2786-4952-2024-1(35)-34-45).
- Nykyporets S. S., Melnyk O. D., Ibrahimova L. V., Boiko Yu. V., Kukharchuk H. V. Fostering critical thinking in technical university students in foreign language classes: strategies and approaches for cultivating analytical proficiency. *Bulletin of Science and Education. Series "Pedagogy"*. 2023. № 8(14). C.344–360. [https://doi.org/10.52058/2786-6165-2023-8\(14\)-344-360](https://doi.org/10.52058/2786-6165-2023-8(14)-344-360).
- Nykyporets S., Stepanova I., Hadaichuk N. The use of Open Educational Resources in Ukraine: unleashing the potential for knowledge democratization and lifelong learning. *Journal of Innovations and Sustainability*. 2023. № 7(1). DOI: <https://doi.org/10.51599/is.2023.07.01.07>.
- Nykyporets S. S., Ibrahimova L. V. An empirical analysis of active and interactive pedagogical strategies in the context of distance learning environments: a comparative study. *Innovations in the Education of the Future: Integration of Humanities, Technical and Natural Sciences: International collective monograph*. FIT CTU in Prague, 2023. Chap. 22. P. 393–410. DOI: <https://doi.org/10.5281/zenodo.10260124>.
- Nykyporets S. S., Stepanova I., Hadaichuk N. Tools and techniques to develop higher order thinking skills in students of non-linguistic technical universities of Ukraine during online learning. *Norwegian Journal of Development of the International Science*. 2023. № 1117. P. 44–49. DOI: <https://doi.org/10.5281/zenodo.8385809>.
- Fedoriv Ya. English for resilience : [comprehensive coursebook] / Fedoriv Ya. R., Finogina T. S., Pirozhenko I. D. ; The National University of “Kyiv-Mohyla Academy”, English Language Department. – Kyiv : National University of “Kyiv-Mohyla Academy”, 2023. – 106 p. URL: <https://ekmair.ukma.edu.ua/handle/123456789/25569>
- Civil society, human rights, and democracy : English for NGOs : student’s book / [course developers: Oksana Kharchenko, Nataliia Sytnyk, Fredric Larsson, Sofiia Kryshtal, Mariia Ivanova]. Kyiv : [s. n.], 2019. 223 p. <https://surl.li/tzcppk> (Accessed on: 5.03.2025).
- Cultural Bridge. Round 2. Evaluation Report 2024 / By TIALT. URL: <https://surl.li/ikogpm> (Accessed on: 5.03.2025).
- Vinnitsia Technical University will cooperate with GlobalLogic. GlobalLogic. URL: <https://surl.li/cacubi> (Accessed on: 5.03.2025).

CHAPTER 16. REGARDING THE ISSUE OF THE PROVISION OF MUNICIPAL SERVICES BY LOCAL GOVERNMENTS

Anatoliy TERLETSKII

Doctor of philosophy, Lecturer of the Department of State and Legal Disciplines

Odessa State University of Internal Affairs

anatoliyterletskii@gmail.com

<https://orcid.org/0009-0000-4767-9768>

Abstract The study is devoted to the problems of providing quality municipal services by local governments at the present stage. The effectiveness and quality of municipal services are measured by the following parameters: the population's assessment of the socio-economic situation; the state of the ecological environment; satisfaction with the work of public transport, the condition of roads, and the improvement of the territory; the protection of public order; the level of public services. Planning for the development of territorial communities should be oriented towards meeting identified needs.

The parameter that determines the quality of municipal services to the population is targeting, because local self-government differs from state administration in its targeting nature. To do this, it is necessary to build a modern quality management system in the process of providing municipal services based on a flexible organizational system for managing territorial communities, improving the level of qualification and competence of managerial personnel, and developing an information system for providing services.

Keywords: administrative services, municipal services, organs of local self-government, administratively is the legal adjusting, digital technologies

1. Administrative and legal regulation of the provision of municipal services by local self-government bodies.

2. Use of digital technologies in the provision of municipal services by local self-government bodies.

ЩОДО ПИТАННЯ НАДАННЯ ОРГАНАМИ МІСЦЕВОГО САМОВРЯДУВАННЯ МУНІЦИПАЛЬНИХ ПОСЛУГ

Анотація Дослідження присвячено проблемам надання якісних муніципальних послуг органами місцевого самоврядування на сучасному етапі. Ефективність і якість надання муніципальних послуг вимірюється такими параметрами: оцінка населенням соціально-економічної ситуації; стан екологічної обстановки; задоволеність роботою громадського транспорту, станом доріг, благоустроєм території; охорона публічного порядку; рівень надання публічних послуг. Планування розвитку територіальних громад має орієнтуватися на задоволення виявлених потреб.

Параметром, що визначає якість муніципальних послуг населенню, є адресність, адже місцеве самоврядування відрізняється від державного управління адресним характером. Для цього необхідно побудувати сучасну систему управління якістю в процесі надання муніципальних послуг на основі гнучкої організаційної системи управління територіальними громадами, підвищення рівня кваліфікації та компетентності управлінських кадрів, розроблення інформаційної системи надання послуг.

Ключові слова: адміністративні послуги, муніципальні послуги, органи місцевого самоврядування, адміністративно-правове регулювання, цифрові технології

1.Адміністративно-правове регулювання надання органами місцевого самоврядування муніципальних послуг.

2. Використання цифрових технологій під час надання муніципальних послуг органами місцевого самоврядування.

Вступ. Надання якісних публічних послуг прямо пов'язується з розвитком України та покращанням добробуту громадян. Саме тому питання надання якісних публічних послуг є надзвичайно актуальним.

На думку дослідників (*Клімушин П. С., Спасібов Д. В., 2017*), у «сервісній державі» існує розвинене громадянське суспільство, і держава має створювати умови для самореалізації особистості, надавати послуги, що задовольняють потреби населення. Саме люди, а не держава впливають на кількість та зміст публічних послуг, а органи публічного адміністрування повинні змінювати свою діяльність під потреби населення.

Діяльність територіальної громади реалізується через систему муніципальних послуг, надання яких органами місцевого самоврядування забезпечує ті чи інші складові якості життя. Управління наданням муніципальних послуг є найважливішою частиною публічного адміністрування, тому питання муніципальних послуг є ключовим для розуміння всіх соціально-економічних процесів, які відбуваються на місцевому рівні (*Терлецький А.В., 2023, с.118*).

Місцеве самоврядування, як зазначає І. Б. Коліушко – це спосіб організації простору проживання громадян, за якого місцевим громадам делеговано право і можливість самостійно вирішувати всі питання місцевого життя, в тому числі питання забезпечення членів громад більшістю публічних послуг, які гарантовані законодавством (освіта, охорона здоров'я, культура, житлово-комунальні та ін. послуги) (*Коліушко І. Б., 1993, с. 74*).

Роль органів місцевого самоврядування полягає в тому, щоб визначити оптимальне співвідношення набору послуг, їх кількості, якості та вартості. При ігноруванні потреб і пріоритетів населення наявні ресурси можуть бути витрачені нерационально (*Терлецький А.В., 2023, с.75*).

Муніципальна послуга як вид публічних послуг є базовим елементом, клітиною муніципальної діяльності, основою економічних і соціальних відносин між людьми в межах територіальної громади. Побудова цілісної системи адміністративно-правового регулювання надання муніципальних послуг – один із найважливіших пріоритетів реформування всієї системи місцевого самоврядування, спрямованого завершення процесів розмежування повноважень між регіональним і муніципальним рівнями управління (*Терлецький А.В., 2024, с.120*).

На сучасному етапі розвитку держави підвищується роль інформаційних технологій. Інформатизація всіх сфер життєдіяльності суспільства, та загалом розвиток держави і суспільства є підставою для перегляду правил і способів функціонування органів, що надають послуги з метою забезпечення доступності їх отримання кожною особою. Найбільш наближеними до громади є муніципальні послуги, однак із запровадженням загальнодержавного застосунку «Дія», отримати деякі загальнодержавні послуги особі стало швидше і зручніше ніж муніципальні послуги.

Цифрова держава – це курс, обраний в рамках державної політики з 2019 року, тож і муніципальні органи мають забезпечувати реалізацію такого курсу, удосконалювати свої функції і забезпечувати доступність отримання муніципальних послуг, обізнаність населення у нових можливостях та способів користуватись ними, що відповідно і потребує додаткового дослідження (Козін А.О., 2024, с. 63).

1.Адміністративно-правове регулювання надання органами місцевого самоврядування муніципальних послуг

В умовах децентралізації влади й розбудови демократичної, правової української держави, в якій пріоритетними питаннями є забезпечення громадянам України європейського рівня життя, особливо актуальними стають дослідження, що проводяться з метою вдосконалення якості надання публічних послуг. По-перше, це дозволить, зрозуміти природу публічної, муніципальної послуги; по-друге, виявити реальну картину з надання послуг, зокрема на муніципальному рівні для подальшого їх вдосконалення; по-третє надання послуг держслужбовцями й посадовими особами місцевого самоврядування має стати складовою їхньої професійної діяльності (Чухарев А.В. (2020), с.2).

Статтею 3 Конституції України визначено, що права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави (7). Утвердження і забезпечення прав і свобод людини є головним обов'язком держави. Реалізувати цей обов'язок держава може певною мірою шляхом надання послуг населенню органами виконавчої влади та органами місцевого самоврядування. Органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, у межах повноважень та в спосіб, що передбачені Конституцією та законами України. У статті 92 Конституції України вказано, що лише законами визначаються засади місцевого самоврядування, тому питання надання муніципальних послуг слід регулювати законодавчо (7).

У Законі України «Про особливості надання публічних (електронних публічних) послуг» (8) надано таке визначення: «Публічна послуга – юридично або соціально значуща дія суб'єкта надання публічної (електронної публічної) послуги, у тому числі адміністративна послуга, за заявою (зверненням, запитом) суб'єкта звернення або без такого звернення, у результаті якої набуваються, переходять, припиняються права та/або здійснюються обов'язки суб'єктом звернення, надаються відповідні матеріальні та/або нематеріальні блага суб'єкту звернення».

Закон України «Про місцеве самоврядування в Україні» розкриває сутність місцевого самоврядування: «реальна здатність територіальних громад безпосередньо та через органи місцевого самоврядування вирішувати питання місцевого значення...» (9).

Процеси розвитку демократії, руху до громадянського суспільства ставлять сьогодні перед органами місцевого самоврядування нагальне завдання – радикально підвищити якість публічних послуг. Прагнення людей до високого рівня та якості життя є сигналом до необхідності вдосконалення системи надання публічних послуг, зміни стилю діяльності місцевої влади. Адекватна відповідь на зазначені виклики є індикатором спроможності влади, її результативності й ефективності, тобто запорукою стабільності в суспільстві. У підписаній у 2015 році Стратегії сталого розвитку «Україна-2020» (10) указано, що метою Стратегії є впровадження в Україні європейських стандартів життя та вихід України на провідні позиції у світі.

Інституту адміністративних послуг присвячено велику кількість праць вчених, зокрема: В.Б. Авер'янова, К.О. Афанасьєва, Л.Р. Біла, Н.П. Бортник, Н.Т. Гончарук, Ю.М. Жук, Г. Г. Забарного, Ю. П. Шарова, Р. А. Калюжного, С.В. Ківалова, А. В. Кірмач, І.Б. Коліушко, М. В. Коваліва, О.В. Кузьменко, А.В. Ліпенцева, Т. В. Мамотової, О. І. Остапенко, В. Л. Ортинського, Л.І. Сопільника, В.П. Тимошука, О.В. Терещука, Х.П. Ярмакі та інших. Зважаючи на значний внесок вчених-адміністративістів в удосконалення інституту адміністративних послуг в Україні, подальшого дослідження потребують муніципальні послуги.

Надання публічних послуг є складовою демократичного дискурсу. При цьому вони багато в чому пояснюють необхідність існування держави і системи державної (публічної) влади. Більше того, дедалі активніше розвивається концепція взаємозв'язку публічних послуг із таким феноменом, як громадянство. Громадянство як стійкий правовий зв'язок людини і держави зумовлює пріоритетне надання послуг «своєму» громадянину з боку держави (Терлецький А.В., 2024, с.31).

У вітчизняній правовій науці адміністративна діяльність із надання послуг, які називають і публічними, і громадськими, і соціальними, і державними, і муніципальними, – стала активно досліджуватися лише в останнє десятиліття. Пізнання природи та сутності муніципальної послуги справедливо пов'язується вітчизняними дослідниками з визначенням її місця в системі публічних послуг. У наукових працях з юриспруденції проводяться теоретико-правові та порівняльно-правові дослідження поняття та особливостей публічних, соціальних, державних та муніципальних послуг, визначається їх спільність та видова відмінність (Венедіктова І., 2009; Голосніченко І. П., Циганов О. Г., Попова О. О. (2015)). Поняття «публічні послуги», «державні послуги», «муніципальні послуги», «соціальні послуги» увійшли в українську дійсність спочатку із зарубіжної економічної науки та були зумовлені реформами системи державного управління в європейських державах у 90-ті рр. XX ст. Значного поширення там набула доктрина публічних послуг, які надаються державою та муніципальними утвореннями, що отримала назву «суспільні блага».

Відповідно до згаданої теорії, блага суспільного користування призначені для загального споживання не поділяються на частини; при задоволенні потреб додаткових споживачів не зменшується рівень задоволення тими самими потребами всіма іншими споживачами (Радіонов Ю.Д., 2017). Науковці у сфері менеджменту називають також інноваційні процеси, що формуються в публічному адмініструванні, «сервісною» моделлю держави (Клімушин П. С., Спаськов Д. В., 2017, с.4; Туркова О. К., 2015, с.191) чи моделлю нової адміністрації як служби гарантованого сервісу (Тищенкова І.О., 2017), які отримали своє становлення за кордоном у країнах англосаксонської правової системи.

Сьогодні у вітчизняній юридичній науці в основному визнається, що категорія «публічні послуги» є більш широкою по відношенню до категорій «державні послуги» та «муніципальні послуги». На думку Панькової З. Л. (Панькова З.Л., 2018), публічні послуги слід визначати як певну діяльність, що спрямована на забезпечення життєво необхідних потреб суспільства в цілому і кожної особи зокрема. На думку Є. О. Легези, в основі надання публічних послуг лежить саме публічний інтерес (Легеза Є.О., 2016, с. 31). В. Б.Авер'янов класифікуючи публічні послуги за суб'єктом їх надання поділяє:

на державні і муніципальні, проте доповнює муніципальні публічні послуги ще й комунальними публічними послугами (*Адміністративне право, 2005, с. 454*).

Під адміністративними муніципальними послугами слід розуміти діяльність сільських, селищних та міських рад (або їх виконавчих органів) із реалізації владних повноважень із метою задоволення потреб фізичних та юридичних осіб в отриманні адміністративного акта (документа) або акту (дії), спрямованого на набуття, зміну чи припинення прав та обов'язків таких осіб відповідно до закону за їхньою заявою. На нашу думку, органи місцевого самоврядування повинні стати основним суб'єктом надання адміністративних послуг, для чого необхідно забезпечити належне матеріальне задоволення та організаційні умови, що потрібні для реалізації органами місцевого самоврядування повноважень із надання муніципальних адміністративних послуг. Це підвищить якість та доступність послуг для споживачів, які звертаються за ними (*Терлецький А.В., 2024, с.97*).

Попередні проблемні питання призводять до невизначеності щодо встановлення особливостей правового регулювання надання відповідних послуг, зокрема, можливості їх урегулювання виключно законом та/або підзаконними нормативно-правовими актами. З одного боку, регулювання окремих питань (у тому числі, тих, врегулювання яких Конституцією України прямо передбачено лише за посередництвом закону) нормами законів передбачає їх (а по суті йдеться про можливості реалізації певних прав) конституційно-правове гарантування, забезпечення і захист.

З іншого боку, якщо йдеться про дотримання певного рівня якості послуг, що надаються, зокрема й тих, що можуть/повинні надаватися відповідними органами місцевого самоврядування, то йдеться про можливість врегулювання окремих питань щодо особливостей надання публічних послуг відповідними органами і посадовими особами місцевого самоврядування. Проте у такому разі постає одразу декілька пов'язаних між собою проблем, як, наприклад, недосконалість і незавершеність процесу децентралізації (зокрема й у питаннях передання відповідних повноважень і фінансових ресурсів); визначення місця актів органів місцевого самоврядування у системі законодавства (що є предметом окремого дослідження); наявність не лише достатніх фінансових, а й інших ресурсів (матеріальної бази, кваліфікованих кадрів та персоналу, оплати праці) тощо (*Терлецький А.В. (2024), с.136*).

Так, за даними порталу «Децентралізація», дуже низькою є інтеграція послуг РАЦС у ЦНАП, ураховуючи життєву важливість цих послуг для громадян, і потребує їх надання в комплексі з іншими послугами за моделлю життєвих ситуацій. Більше того, через відсутність цих повноважень у багатьох органах місцевого самоврядування громадяни змушені витратити час і навіть ризикувати здоров'ям (у поточній ситуації) на поїздки до органів Мін'юсту за елементарною послугою (реєстрація народження, смерті), замість того щоб отримати це у своїй громаді швидко (20).

Наприклад, незважаючи на те, що Законом України «Про адміністративні послуги» (21) передбачено, що державна політика у відповідній сфері повинна базуватися, зокрема, на принципі доступності й зручності для суб'єктів звернення, у цьому акті й досі чітко та повно не визначені обов'язкові вимоги до Центрів, також і вимоги щодо територіальної доступності, мережі територіальних підрозділів та віддалених робочих місць зазначених Центрів, облаштування приміщень тощо. Це ускладнює, а інколи й унеможливує реалізацію в повній мірі прав, свобод і законних

інтересів фізичних та юридичних осіб у сфері надання муніципальних адміністративних послуг, створення відповідних стандартів, проведення вартісної оцінки послуг.

Суттєвим недоліком законодавчого регулювання статусу Центрів є також те, що відповідно до закону послуги надаються не в Центрі, а через (за посередництвом) Центр. Тому цілий комплекс працює переважно на прийом/видачу документів через адміністратора Центру. З огляду на тотальну цифровізацію, таке використання Центрів є нелогічним. А з урахуванням того, що більшість Центрів підключена до основних національних електронних інформаційних ресурсів наявні достатні умови отримати послугу безпосередньо у Центрі. Для громадян надання послуг через Центр, а не у Центрі означає необхідність відвідувати його мінімум двічі (*Терлецький А.В., 2024, с.138*). Законодавче регулювання указаних питань постійне «відстає» від фактичних обставин, що особливо яскраво виявляється на рівні регіонів (зокрема потенційно корупційною сферою є державна реєстрація юридичних осіб і фізичних осіб підприємців).

Водночас спостерігається і зворотний процес: безпідставне випередження, часто пов'язане із необхідністю виконання державою взятих на себе зобов'язань щодо виконання різних міжнародних договорів і угод без урахування реальних можливостей (наприклад, Асоціації з ЄС та ін.), а також надмірна зарегульованість, що породжує додаткові перешкоди для ведення бізнесу і створює передумови для корупції у відповідній сфері. Тому актуальною проблемою є скорочення адміністративного тиску на економіку в цілому, а також оптимізація публічного адміністрування.

2. Використання цифрових технологій під час надання муніципальних послуг органами місцевого самоврядування

Організація надання адміністративних послуг, зокрема в електронній формі, цифрова трансформація цієї сфери визначально впливатимуть на щоденне життя мешканців усіх громад України, а також на роботу публічних службовців. Питання цифрового розвитку, цифрової трансформації та цифровізації нині є одним з пріоритетів у діяльності Кабінету Міністрів України, центральних органів виконавчої влади та багатьох органів місцевого самоврядування. При реформуванні будь-якої сфери треба враховувати релевантний досвід інших країн, постійно відстежувати тенденції, виклики, проблематику задля набуття позитивного досвіду та отримання найліпших результатів. У завданнях Програми «U-LEAD з Європою», відповідно до Угоди між Урядом України та Європейським Союзом, передбачено підготовку пропозицій щодо державної політики у сфері децентралізації та адміністративних послуг, надання відповідної консультативної підтримки Уряду України щодо реформування політики та законодавства (22).

Перелік органів місцевого самоврядування визначений Конституцією України (7) як ради та їх виконавчі органи, і відповідно виконавчі органи здійснюють відповідно до Закону України «Про місцеве самоврядування в Україні» (9) власні та делеговані повноваження, тож муніципальні послуги – це реалізація органами місцевого самоврядування саме делегованих повноважень. Вищезазначена Концепція закріпила напрямки реформування і муніципальних послуг, зокрема, основними принципами послуги закріплено доступність послуг та їх відкритість.

Однак, вищезазначена Концепція не передбачала у контексті доступності забезпечення отримання муніципальної послуги з використанням цифрових

технологій, а було передбачено лише правило «єдиного вікна», тобто отримання всіх послуг у одному місці. Цьому принципу наразі відповідають центри надання адміністративних послуг (далі- ЦНАП), що створені майже при кожній адміністрації у містах та обласних центрах. Постійно діючими органами або підрозділами органів місцевого самоврядування, що надають адміністративні послуги через адміністратора шляхом його взаємодії з суб'єктами надання адміністративних послуг відповідно до статті 12 Закону України «Про адміністративні послуги» є центри надання адміністративних послуг (21). Близько 1000 територіальних громад станом на кінець 2022 року отримують необхідні послуги через центри надання адміністративних послуг, яких налічується 3142 (Рабчинська Л., 2022).

У зв'язку із глобальною цифровою революцією використання цифрових технологій у сфері надання послуг державою стало поширеною практикою багатьох високорозвинених держав світу. Використовуючи позитивний досвід європейських країн, зокрема Грузії, Республіки Польща, Німеччини, Україна започаткувала і власні ініціативи щодо впровадження цифрових технологій у сфері надання адміністративних послуг. В Україні для проведення цифрової трансформації у сфері державного управління, зокрема в галузі надання адміністративних послуг, створено Міністерство цифрової трансформації України (Крикавська І., 2020, с. 163).

Розвиток цифрової (електронної) послуги в Україні, розпочався у 2015 році зі створення профільного структурного підрозділу Київської міської державної адміністрації, – Департаменту інформаційно-комунікаційних технологій.

Разом зі структурними змінами у цей період затверджувались муніципальні програми у сфері ІТ, які дозволяли користуватись електронними муніципальними послугами, на кшталт електронних квитків у муніципальному транспорті тощо.

За період 2015 – 2020 років було створено систему електронного урядування (E-government), яка забезпечила впровадження електронного документообігу для взаємодії всіх державних органів з громадянами; через персональні електронні кабінети та цифровий підпис громадяни отримали безпосередній доступ до державних органів і публічних реєстрів, що дозволило подавати документи в електронному форматі, відстежувати їхній статус та скоротити час на їхній розгляд, усунувши людський фактор; проведено аналіз трудовитрат для виконання робочих процесів, що стало основою для впровадження рішень щодо автоматизації та оптимізації цих процесів; на основі технологій Big Data та штучного інтелекту стало можливим ухвалення рішень без участі людини; оцифровано процеси видачі дозволів і ліцензій, що сприяло створенню рівних умов для ведення бізнесу та мінімізації корупційних ризиків. На нашу думку, зазначені аспекти є надзвичайно позитивними як в цілому для побудови якісної та ефективної системи електронного урядування в цілому так і для функціонування ЦНАП (Гульчук Є.О., 2021).

У процесі цифровізації ЦНАП використовуються різноманітні електронні інструменти, серед яких варто виділити системи електронного документообігу, електронні черги, онлайн-послуги та мобільні додатки. Система електронного документообігу дає змогу зменшити використання паперових документів, прискорюючи обробку інформації між різними відділами, що знижує адміністративне навантаження. Електронні черги допомагають організувати візити громадян заздалегідь, мінімізуючи час очікування. Онлайн-сервіси та мобільні додатки дозволяють отримувати

адміністративні послуги дистанційно, що є особливо важливим для жителів віддалених районів і громадян з обмеженими можливостями (Тимошук В., 2015).

Цифровізація діяльності ЦНАП має очевидні переваги як для держави, так і для громадян.

По-перше, вона покращує доступність послуг, оскільки громадяни можуть скористатися ними в будь-який зручний час, не виходячи з дому.

По-друге, автоматизовані процеси забезпечують швидке обслуговування, мінімізують кількість помилок і пришвидшують виконання запитів.

По-третє, використання цифрових технологій знижує ризики корупції через мінімізацію впливу людського фактора на прийняття рішень, що підвищує прозорість роботи ЦНАП і сприяє зміцненню довіри до державних установ (Гульчук Є.О., 2021, с.198).

Нарешті, цифровізація дозволяє економити бюджетні кошти шляхом зниження витрат на паперовий документообіг та зменшення адміністративних витрат.

Незважаючи на численні переваги, процес цифровізації ЦНАП супроводжується і значними викликами. Перш за все, це забезпечення надійного захисту персональних даних громадян, оскільки зростання обсягу цифрової інформації потребує додаткових заходів для збереження конфіденційності та безпеки.

Другим важливим аспектом є технічне оснащення ЦНАП і доступ до якісного інтернет-зв'язку, що особливо актуально для віддалених регіонів з обмеженими ресурсами. Крім того, впровадження нових технологій вимагає підвищення кваліфікації працівників центрів, які мають володіти необхідними навичками для роботи з цифровими інструментами, що потребує впровадження програм навчання та перепідготовки. Вудмітимо, що цифровізація ЦНАП є важливим кроком до підвищення ефективності, прозорості та зручності державних послуг в Україні.

З одного боку, успішне впровадження цифрових технологій сприяє покращенню взаємодії громадян з державою та зменшує бюрократичні бар'єри, а з іншого – вимагає подолання низки викликів, серед яких головними є забезпечення правової підтримки, безпеки даних, доступності технічних ресурсів і підготовки персоналу (Гульчук Є.О., 2021, с.199).

Оцифрування сервісів надання адміністративних послуг сприймається населенням як ознака зручності й доступності послуг, виявлення до них лояльності та турботи. Згідно з соціологічними дослідженнями «Оцінки населенням України якості надання адміністративних послуг» проведеного Фондом «Демократичні ініціативи» імені Ілька Кучеріва спільно з соціологічною службою Центру Разумкова, від 12 до 17 липня 2019 року 5 % населення хоча б раз скористалися адміністративними послугами он-лайн. Найбільш популярними серед респондентів виявилися цифрові сервіси таких державних установ: Міністерства соціальної політики (47,4 % респондентів), Міністерства юстиції (30,3 % респондентів), Державної фіскальної служби (22,6 % респондентів)(27).

Із запровадженням загальнодержавного застосунку «Дія» електронні послуги почали надаватись за допомогою цього застосунку, в електронній формі. Більшість адміністративних послуг люди в Україні можуть отримати, використавши зазначений застосунок, однак не всі муніципальні послуги до нього включені. Станом на вересень 2021 року послуги у застосунку Дія розширили та внесли муніципальні послуги (28).

Електронні послуги як результат пропонують не лише документ, а і дію, однак етапність виконання здебільшого збігається. Відповідно до розпорядження Кабінету Міністрів України «Деякі питання надання адміністративних послуг органів виконавчої влади через центри надання адміністративних послуг» до переліку адміністративних послуг внесли адміністративні послуги, що надаються органами місцевого самоврядування у порядку виконання делегованих повноважень, зокрема, такі як послуги державних адміністрацій та територіальних органів, центральних органів виконавчої влади з питань соціального захисту, діяльності бізнесу та громадських формувань, земельних та екологічних питань, питань будівництва та нерухомості, транспорту, громадянства та міграції, освіти, спорту, туризму, релігії і культури, безпеки життєдіяльності, виробництва та обігу окремих видів продукції тощо (29).

Підставою відповідних змін стало прийняття законодавства щодо оптимізації функціонування центрів надання послуг та спрощення надання адміністративних послуг, суб'єктом надання яких є орган місцевого самоврядування, якщо така послуга здійснюється через зазначений центр надання адміністративних послуг (30).

Веб-портали і центри надання адміністративних послуг є ефективними інструментами надання муніципальних послуг, однак наступним кроком реформування адміністративних послуг є використання штучного інтелекту під час надання адміністративної послуги.

Зокрема, дослідження науковців у сфері використання штучного інтелекту під час функціонування органів державної влади чи місцевого самоврядування вже відбувається, зокрема, в межах таких досліджень пропонується розробляти технології на благо людства з використанням штучного інтелекту при створенні нових програм, зокрема програм забезпечення надання електронних послуг (*Yara O., Brazheyev A., Golovko L., Bashkatova V., 2021, c. 287*).

Для оцінювання електронних послуг створюються міжнародні онлайн-опитування в мережах Інтернет. Розвиненою система надання електронних послуг вважається у Сполучених Штатах Америки, де більшість державних веб-сайтів проводять опитування та надають максимум електронних послуг. (32).

Результати міжнародних рейтингів онлайн-опитувань, щодо надання муніципальних послуг показали, що Данія, Фінляндія та Нідерланди мають найвищі показники надання муніципальних послуг – більш ніж 90% (33).

За міжнародний рейтингом EGDІ за показником цифровізації послуг найкращі показники має Данія. Досвід Данії є перспективним для використання Україною, адже кожен мешканець Данії має онлайн кабінет, за допомогою якого отримає інформацію від представників державних органів та органів місцевого самоврядування: отримує роз'яснення, послуги тощо (*Туркова О. К., 2015*).

У процесі розвитку центрів надання муніципальних послуг в Україні важливою складовою є їх адаптація до умов цифровізації, що дозволяє значно покращити ефективність взаємодії між громадянами та органами державної влади. Інтеграція цифрових технологій забезпечує оперативність, зручність та прозорість надання послуг, що особливо важливо для підвищення довіри населення до державних інститутів.

Безумовно, використання цифрових технологій у сфері надання послуг органами місцевого самоврядування потребує формування інноваційного нормативно-

правового забезпечення такої діяльності, а також вдосконалення та розширення існуючої нормативної бази.

Муніципальні послуги перебувають у процесі активного переходу у електронну форму їх надання. Державна політика формується у напрямку стимулювання розвитку надання електронних послуг органами місцевого самоврядування, адже їх кількість на веб-порталі «Дія» лише збільшується з часом.

Закони і підзаконні нормативно-правові акти також прописані лише на користь розвитку електронних муніципальних послуг. Надання електронних послуг оптимізує витрати з державного та місцевого бюджетів, скорочує кадровий голод та не створює перешкод особи у отриманні послуги за принципом «тут і зараз», розвиває інформаційно-комунікаційні навички громадян та позитивно впливає на готовність громадян до змін.

Важливим напрямом оцифрування надання адміністративних послуг населенню є проведення нормативно врегульованих заходів, що сприятимуть освоєнню новітніх інформаційно-комунікаційних технологій як посадовими особами, які надають послуги, так і отримувачами послуг.

Висновки. Важливим аспектом удосконалення надання муніципальних послуг є не тільки наявність достатніх фінансових, матеріальних і технічних ресурсів, але й наявність кваліфікованих працівників та менеджерів, що забезпечуватимуть ефективне їх розподілення та використання, а тому формування кадрового потенціалу з ухилом на діяльність з обслуговування громадян повинні виноситися на перший план і контролюватися на усіх етапах впровадження реформи децентралізації.

Під час надання органами місцевого самоврядування муніципальних послуг доцільно враховувати думку населення та оцінювати ефективність і якість муніципальних послуг.

Нормами Закону України «Про адміністративні послуги» передбачено, що державна політика у відповідній сфері повинна базуватися, зокрема, на принципі доступності й зручності для суб'єктів звернення. Норми вказаного закону чітко та повно не визначені обов'язкові вимоги до Центрів надання послуг, також і вимоги щодо територіальної доступності, мережі територіальних підрозділів та віддалених робочих місць зазначених Центрів, облаштування приміщень тощо. Це ускладнює, а інколи й унеможлиблює реалізацію в повній мірі прав, свобод і законних інтересів фізичних та юридичних осіб у сфері надання муніципальних адміністративних послуг, створення відповідних стандартів, проведення вартісної оцінки послуг.

Аналіз надання муніципальних послуг дає можливість заключити: параметром, що визначає якість муніципальних послуг населенню, є адресність, адже місцеве самоврядування відрізняється від державного управління адресним характером.

Підвищити якість надання муніципальних послуг споживачам можливо із запровадженням міжнародних стандартів системи управління якістю. Для цього необхідно побудувати сучасну систему управління якістю в процесі надання муніципальних послуг на основі гнучкої організаційної системи управління територіальними громадами, підвищення рівня кваліфікації та компетентності управлінських кадрів, розроблення інформаційної системи надання послуг в місцевих органах влади.

Запорукою високих вимог до якості муніципальних послуг має стати належним чином організований процес надання послуг, а також використання статистичних методів його контролю, і, відповідно, постійне вдосконалення процесу з метою підвищення якості послуг.

Приклад Данії є перспективним для використання Україною, адже кожен данський мешканець має онлайн кабінет, за допомогою якого спілкується з представниками державних органів та органів місцевого самоврядування: отримує роз'яснення, послуги тощо.

Цифровізація центрів надання адміністративних послуг є важливим кроком до підвищення ефективності, доступності та прозорості муніципальних послуг. Впровадження електронних сервісів та автоматизація процесів дозволяють знизити навантаження, зменшити час обслуговування громадян та знизити рівень корупції.

Одним із перспективних кроків у розвитку надання муніципальних електронних послуг є використання штучного інтелекту.

References:

- Клімушин П. С., Спасібов Д. В. (2017) Концепція сервісно орієнтованої держави в контексті модернізації публічного управління. Теорія та практика державного управління. 2017. № 2(57). С. 3–8. URL: <https://surli.cc/iudhun>
- Терлецький А.В. (2023) Проблеми правового регулювання надання органами місцевого самоврядування муніципальних послуг. Юридичний науковий електронний журнал 2023. №11. С.118-121. URL: http://www.lsej.org.ua/11_2023/26.pdf
- Коліушко І.Б. (1993) До конституційного закріплення територіального устрою. Актуальні проблеми управління територіями в Україні : матеріали наук.-практ. конф. (Київ, 26–27 листоп. 1992 р.). К., 1993. С. 74–77.
- Терлецький А.В. (2024) Адміністративно-правові засади діяльності органів місцевого самоврядування з надання муніципальних послуг в Україні. дис.... на здобуття наукового ступеня доктора філософії. спец. 081 право. Одеса. 2024. 213с. URL: <https://uacademic.info/ua/document/0824U000951>
- Козін А.О. (2024) Забезпечення доступності муніципальних послуг шляхом використання цифрових технологій. Київський часопис права. 2024 №3. С.62-66. DOI: <https://doi.org/10.32782/klj/2024.3.9>
- Чухарев А.В. (2020) Підвищення якості муніципальних послуг в умовах децентралізації. автор. маг. роботи на здобуття наук. ступ. магістра публічного управління спец.: 281 Миколаїв. 2020. 14с. URL: <https://krs.chmnu.edu.ua/jspui/handle/123456789/1529>
- Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 черв. 1996 р. Відомості Верховної Ради України. 1996. № 30.
- Про особливості надання публічних (електронних публічних) послуг: Закон України від 15 липня 2021 р. № 1689-IX. Відомості Верховної Ради. 2021. № 47. Ст. 383.
- Про місцеве самоврядування в Україні: Закон України від 21.05.1997 № 280/97-ВР. Урядовий кур'єр. 1997. 14 червня.
- Про Стратегію сталого розвитку «Україна–2020» : Указ Президента України від 12 січня 2015 року № 5/2015.
- Венедіктова І. (2009) Юридична природа публічних послуг. Вісник Харківського національного університету. 2009. № 841. С. 88–91.
- Адміністративні послуги у сфері внутрішніх справ (2015) : монографія / І. П. Голосніченко, О. Г. Циганов, О. О. Попова [та інші]; К. : НТУУ «КПІ», 2015. 590 с. URL: <https://ela.kpi.ua/handle/123456789/11974>
- Терлецький А.В. (2023) Якість муніципальних послуг як об'єкт оцінки та управління. Публічне право 2023. №3(51). С.73-81. URL: <https://publichne-pravo.com.ua/files/51/8.pdf>

- Радіонов Ю.Д. (2017) Теорія виробництва і надання суспільних благ. Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство. 2017. Вип. 11. С. 129–133. URL: <https://dspace.uzhnu.edu.ua/jspui/handle/lib/13833>
- Туркова О. К. (2015) Сервісна спрямованість надання адміністративних послуг в Україні: процедурні аспекти. Право і суспільство. 2015. № 5/2, ч. 3. С. 189–194. URL: <https://clar.navs.edu.ua/handle/123456789/34335>
- Тищенко І.О. (2017) Електронні послуги у діяльності публічної адміністрації України: монограф. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2017. 156 с. URL: <https://er.dduvs.edu.ua/bitstream/123456789/935/1>
- Панькова З.Л. (2018) Адміністративні послуги у сфері економіки. дис. ... канд. ю. н. Київ, 2018. 225 с. URL: [https://doi.org/10.20535/2308-5053.2018.3\(39\).193812](https://doi.org/10.20535/2308-5053.2018.3(39).193812)
- Легеза Є.О. (2016) Теорія публічних послуг: адміністративно-правова складова : монографія Херсон : Вид. дім «Гельветика», 2016. 452 с.
- Адміністративне право. (2005) Академічний курс: підруч.: у 2 т. / ред. колегія: В. Б. Авер'янов (голова) та ін. К.: Юрид. думка, 2005. Т. 2. Особлива частина. 625 с.
- Петришина М.О. (2020) Теоретико-правові проблеми забезпечення надання публічних послуг суб'єктам господарювання органами місцевого самоврядування. Право та інновації. 2020. № 2 (30). С. 93–98. URL: <https://surl.li/eirniw>
- Про адміністративні послуги: Закон України від 06.09.2012 № 5203-VI. Голос України від 06.10.2012 № 188.
- Пропозиції щодо окремих напрямків державної політики з цифрової трансформації сфери надання адміністративних послуг та ЦНАП. 2021. URL: <https://surl.li/gkxysh>
- Рабчинська Л. (2022) Що покращилося у Центрах надання адміністративних послуг. URL: <https://www.pravda.com.ua/columns/2022/02/24/7325177>
- Крикавська І. (2020) Нормативно-правове регулювання впровадження та використання цифрових технологій у сфері надання адміністративних послуг Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки» 2020. № 2, Т.7. С. 162-165.
- Гульчук Є.О. (2021) Діяльність центрів надання адміністративних послуг в умовах цифровізації. Держава та регіони. Серія: Право. 2021 №2(72) С.197-201.
- Тимошук В. (2015) Надання адміністративних послуг у муніципальному секторі: Навчальний посібник для посадових осіб місцевого самоврядування. Асоціація міст України. К., ТОВ «Підприємство «ВІ ЕН ЕЙ». 2015. 124 с.
- Діджиталізація сервісів. URL: <https://surl.li/qyeovyn>
- Розширення переліку адміністративних послуг у ЦНАП. URL: <https://surl.li/agaama>
- Деякі питання надання адміністративних послуг органів виконавчої влади через центри надання адміністративних послуг: Розпорядження Кабінету Міністрів України від 16 травня 2014 р. № 523 URL: <https://surl.li/ccmgaufig>
- Про внесення змін до деяких законодавчих актів України щодо оптимізації мережі та функціонування центрів надання адміністративних послуг та удосконалення доступу до адміністративних послуг, які надаються в електронній формі: Закон України від 03.11.2020 № 943-IX. URL: <https://surl.li/wttav1>
- Yara O., Brazheyev A., Golovko L., Bashkatova V. (2021) Legal Regulation of the Use of Artificial Intelligence: Problems and Development Prospects. European Journal of Sustainable Development. 2021. № 10 (1). P. 281-289.
- Does E-Government Improve Government Capacity? Evidence from Tax Administration and Public Procurement. Development Economics 2016 World Development Report Team. 2016. URL: <https://surl.li/nzqmlz>
- E-Government Development Index (EGDI). URL: <https://surl.li/natwtj>
- Чукот С. А., Полярна В. Л. (2016) Основні напрями та пріоритети надання електронних послуг в країнах європейського союзу: на прикладі Данії. Державне управління: удосконалення та розвиток. 2016. № 12. URL: <https://surl.li/fjgyes>

CONTENTS

CHAPTER 1. FORMATION OF A MECHANISM FOR STRATEGIC PLANNING AND MANAGEMENT OF SUSTAINABLE DEVELOPMENT OF AN INDUSTRIAL ENTERPRISE.....	6
CHAPTER 2. INTERNATIONAL COMMERCIAL ARBITRATION IN THE DIGITAL AGE: PROSPECTS AND INFORMATION SECURITY.....	33
CHAPTER 3.	57
CHAPTER 4. MODERN BASES OF FORMING AND ENSURING CYBERSECURITY AS A BASIS OF NATIONAL SECURITY: INTERNATIONAL PRACTICES.....	93
CHAPTER 5. INNOVATIONS IN OCCUPATIONAL HEALTH AND SAFETY.....	114
CHAPTER 6. COMPETENCE-BASED APPROACH IN EDUCATIONAL MANAGEMENT: THEORY AND PRACTICE.....	136
CHAPTER 7. DIGITAL ECONOMY AND INFORMATION SECURITY IN INTERNATIONAL SECURITY SYSTEMS.....	194
CHAPTER 8. REGULATION OF INNOVATIVE DEVELOPMENT OF THE AGRARIAN SECTOR OF THE ECONOMY OF UKRAINE.....	217
CHAPTER 9. COMPLIANCE CONTROL AS A TOOL FOR ENSURING ECONOMIC SECURITY IN THE CORPORATE GOVERNANCE SYSTEM.....	243
CHAPTER 10. TAX POTENTIAL FOR FORMING LOCAL BUDGET REVENUES.....	269
CHAPTER 11. DIGITALIZATION OF PUBLIC AUTHORITY SERVICES AND THE PUBLIC SECTOR OF UKRAINE: STATE, TECHNOLOGIES, AND CHALLENGES.....	296
CHAPTER 12. INFORMATION SECURITY IN THE GLOBAL CONTEXT: LINGUISTIC PERSPECTIVES AND THE ROLE OF ENGLISH.....	321

CHAPTER 13. ECONOMIC SECURITY OF UKRAINE IN THE CONTEXT OF A FULL-SCALE WAR..... 346

CHAPTER 14. THE ROLE OF COMPUTER VISUALIZATION IN THE FORMATION OF MEDIA LITERACY: HOW DIGITAL IMAGES INFLUENCE OUR PERCEPTION OF INFORMATION..... 373

CHAPTER 15. INTERCULTURAL COMMUNICATION IN INFORMATION SECURITY: RISKS, CONFLICTS, AND EDUCATIONAL OPPORTUNITIES FOR ENGLISH LANGUAGE TEACHERS..... 398

CHAPTER 16. REGARDING THE ISSUE OF THE PROVISION OF MUNICIPAL SERVICES BY LOCAL GOVERNMENTS..... 421

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

*International
collective
monograph.
Volume II.*

Підписано до друку 09.05.2025. Формат 70×100 ¹/₁₆
Ум. друк. арк. 27,3. Обл.-вид. арк. 26,8. Зам. 204. Тираж 100.
Папір офсетний. Гарнітура Times. Друк цифровий.

Видавець і виготовлювач ФОП Мажула Ю. М.
43021, м. Луцьк, вул. Винниченка, 47/35.
Тел. моб. 096 61 66 277, e-mail: y.mazhula@gmail.com

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців,
виготовлювачів і розповсюджувачів видавничої продукції
серія ДК № 7662 від 07 вересня 2022 року

M 58 **International security studies: managerial, technical, legal, environmental, informative and psychological aspects.** International collective monograph. Volume II. ISAP, Research and Education. 2025. – 436 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 978-83-8011-444-7

© ISAP 2025;
© The collective of authors 2025

External resources

Indexed in



OpenAIRE



Copyright NIFU: CC BY 4.0