Edited by
Serhii Yevseiev,
Volodymyr Ponomarenko,
Oleksandr Laptiev,
Oleksandr Milov

SYNERGY
OF BUILDING CYBERSECURITY SYSTEMS

Monograph

Technology
Center

2021

UDC 004.056
S98

Published in 2021
by PC TECHNOLOGY CENTER
Shatylova dacha str., 4, Kharkiv, Ukraine, 61165

Approved by the Academic Council of Simon Kuznets Kharkiv National University of Economics, Protocol No. 3 of 15.03.2021

Reviewers:
Nataliia Lukova-Chuiko, Doctor of Technical Science, Head of the Department of Cybersecurity and Information Protection of Taras Shevchenko National University of Kyiv;
Korchenko Alexandr, Doctor of Technical Sciences, Professor, Head of the Department of Information Technology Security of National Aviation University.

S98 **Authors:**
Edited by **Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov**
Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.

ISBN 978-617-7319-31-2 (on-line)
ISBN 978-617-7319-32-9 (print)

The monograph discusses the main types of models used in modeling the behavior of intelligent agents. The originality of the approach associated with the introduction into consideration of the concept of the contour of business processes as an integral object to be protected. The idea of the spatio-temporal structure of the model basis was proposed by the authors, that reflects not only the distribution of the set of models over the corresponding levels of the proposed methodology, but also sets the sequence of their interaction. The application of the developed models to ensure the protection of information and user data in social networks will allow a new look at existing social networks and create new social networks that will provide more reliable security of user data while maintaining usage parameters.
The monograph is intended for teachers, researchers and engineers involved in information security research.
Figures 65, Tables 26, References 155 items.

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.
Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

DOI: 10.15587/978-617-7319-31-2
ISBN 978-617-7319-31-2 (on-line)
ISBN 978-617-7319-32-9 (print)

9 786177 319312

AUTHORS

SERHII YEVSEIEV

Doctor of Technical Science, Professor
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ID ORCID: https://orcid.org/0000-0003-1647-6444

VOLODYMIR PONOMARENKO

Doctor of Economics, Professor
Honored Worker of Science and Technology of Ukraine
Cavalier of the Order of Merit, III, II degrees,
«Order of Prince Yaroslav the Wise» V degree,
corresponding member of the Academy of Pedagogical Sciences of Ukraine
Rector Simon Kuznets Kharkiv National University of Economics
ID ORCID: https://orcid.org/0000-0002-9702-8469

OLEKSANDR LAPTIEV

Doctor of Technical Science, Professor,
Senior Researcher
Department of Information and Cybersecurity Systems
Educational-scientific Institute of Information security
State University of Telecommunications
ID ORCID: https://orcid.org/0000-0002-4194-402X

OLEKSANDR MILOV

Doctor of Technical Science, Professor
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ID ORCID: https://orcid.org/0000-0001-6135-2120

OLHA KOROL

PhD, Associate Professor
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ID ORCID: https://orcid.org/0000-0002-8733-9984

STANISLAV MILEVSKYI

PhD, Associate Professor
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ID ORCID: https://orcid.org/0000-0001-5087-7036

SERHII POHASII

PhD, Associate Professor
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ID ORCID: https://orcid.org/0000-0002-4540-3693

ANDREY TKACHOV

PhD, Senior Researcher
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ID ORCID: https://orcid.org/0000-0003-1428-0173

OLEXANDER SHMATKO

PhD, Associate Professor
Department of Software Engineering and
Management Information Technologies
National Technical University «Kharkiv Polytechnic Institute»
ID ORCID: https://orcid.org/0000-0002-2426-900X

YEVGEN MELENTI

PhD
Department of Tactical, fire and special physical training
Juridical Personnel Training Institute for the Security Service of Ukraine
Yaroslav Mudryi National Law University
ID ORCID: https://orcid.org/0000-0003-2955-2469

OLEKSANDR SIEVIERINOV

PhD, Associate Professor
Department of Information Technologies Security
Kharkiv National University of Radio Electronics
ID ORCID: https://orcid.org/0000-0002-6327-6405

SERGEY OSTAPOV

Doctor of Physics and Mathematics, Professor
Department of Computer Systems Software
Yuriy Fedkovych Chernivtsi National University
ID ORCID: https://orcid.org/0000-0002-4139-4152

ALLA GAVRILOVA

Senior Lecturer
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ID ORCID: https://orcid.org/0000-0002-2015-8927

OLEKSII TSYHANENKO

Postgraduate Student
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ID ORCID: https://orcid.org/0000-0002-5784-8438

SERGEY HERASIMOV

Doctor of Technical Sciences, Professor
Department of Combat Use of Weapons of Air Defense of Ground Forces
Ivan Kozhedub Kharkiv National Air Force University
ID ORCID: https://orcid.org/0000-0003-1810-0387

ELENA NYEMKOVA

Doctor of Technical Sciences, Associate Professor
Department of Information Technology Security
National University Lviv Polytechnic
ID ORCID: https://orcid.org/0000-0003-0690-2657

BOGDAN TOMASHEVSKY

PhD, Associate Professor
Department of Cyber Security
Ternopil Ivan Puluj National Technical University
ID ORCID: https://orcid.org/0000-0002-1934-4773

IVAN GROD

Doctor of Physics and Mathematics, Associate Professor
Department of Cybersecurity
Ternopil Ivan Puluj National Technical University
ID ORCID: https://orcid.org/0000-0002-0678-1456

IVAN OPIRSKYY

Doctor of Technical Science, Professor
Department of Information Security
Lviv Polytechnic National University
ID ORCID: https://orcid.org/0000-0002-8461-8996

VOLODYMYR ZVIERIEV

PhD, Senior Researcher
Department of Software Engineering and Cybersecurity
Kyiv National University of Trade and Economics
ID ORCID: https://orcid.org/0000-0002-0907-0705

OLEKSANDR PROKOPENKO

Postgraduate Student
Center for Military and Strategic Studies
National Defence University of Ukraine named after Ivan Cherniakhovskyi
ID ORCID: https://orcid.org/0000-0002-5482-0317

VITALII SAVCHENKO

Doctor of Technical Sciences, Professor, Director of Institute
Educational-scientific Institute of Information Security
State University of Telecommunications
ID ORCID: https://orcid.org/0000-0002-3014-131X

OLEG BARABASH

Doctor of Technical Sciences, Professor
Department of Automation of Designing of Energy Processes and System
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»
ID ORCID: https://orcid.org/0000-0003-1715-0761

VALENTYN SOBCHUK

Doctor of Technical Sciences, Associate Professor
Department of Higher Mathematics
State University of Telecommunications
ID ORCID: https://orcid.org/0000-0002-4002-8206

GERMAN SHUKLIN

PhD, Head of Department
Department of Information and Cybersecurity Systems
Educational-scientific Institute of Information security
State University of Telecommunications
ID ORCID: https://orcid.org/0000-0003-2507-384X

VLADYSLAV KHVOSTENKO

PhD, Associate Professor, Patent Attorney of Ukraine
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ID ORCID: https://orcid.org/0000-0002-6436-4159

OLEKSANDR TYMOCHKO

Doctor of Technical Sciences, Professor
Department of Air Navigation and Combat Control of Aviation
Ivan Kozhedub Kharkiv National Air Force University
ID ORCID: https://orcid.org/0000-0002-4154-7876

MAKSIM PAVLENKO

Doctor of Technical Sciences, Associate Professor, Head of Department
Department of Mathematical and Software of Automated Control Systems
Ivan Kozhedub Kharkiv National Air Force University
ID ORCID: https://orcid.org/0000-0003-3216-1864

ANDRII TRYSTAN

Doctor of Technical Sciences, Senior Research, Head of Department
Department of Air Force Science Center
Ivan Kozhedub Kharkiv National Air Force University
ID ORCID: https://orcid.org/0000-0002-2137-5712

SERHII FLOROV

Associate Professor, Full Member of the Ukrainian Academy of Cybersecurity
Department of Cybersecurity and Telecommunications
National Technical University Dnipro Polytechnic
ID ORCID: https://orcid.org/0000-0002-4682-7666

ABSTRACT

The development of the modern world community is closely related to advances in computing resources and cyberspace. The formation and expansion of the range of services is based on the achievements of mankind in the field of high technologies. However, the rapid growth of computing resources, the emergence of a full-scale quantum computer tightens the requirements for security systems not only for information and communication systems, but also for cyber-physical systems and technologies.

The methodological foundations of building security systems for critical infrastructure facilities based on modeling the processes of behavior of antagonistic agents in security systems are discussed in the first chapter.

The concept of information security in social networks, based on mathematical models of data protection, taking into account the influence of specific parameters of the social network, the effects on the network are proposed in second chapter.

The nonlinear relationships of the parameters of the defense system, attacks, social networks, as well as the influence of individual characteristics of users and the nature of the relationships between them, takes into account.

In the third section, practical aspects of the methodology for constructing post-quantum algorithms for asymmetric McEliece and Niederreiter cryptosystems on algebraic codes (elliptic and modified elliptic codes), their mathematical models and practical algorithms are considered. Hybrid crypto-code constructions of McEliece and Niederreiter on defective codes are proposed. They can significantly reduce the energy costs for implementation, while ensuring the required level of cryptographic strength of the system as a whole. The concept of security of corporate information and educational systems based on the construction of an adaptive information security system is proposed.

KEYWORDS

Cybersecurity, modeling of conflict-cooperative interaction, crypto-code constructions, algebraic geometric codes, classifiers of cyber threats.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

CIRCLE OF READERS AND SCOPE OF APPLICATION

The authors propose new approaches to the problem of information security in the monograph. The new approach is based on the detection of threats to all components of security: cybersecurity, information security and security of information, synergy and hybridity of modern threats.

The first section discusses the main types of models used in modeling the behavior of intelligent agents. A distinctive feature is that not only the main classes of models are considered, but also the main directions of research of behavioral processes. The joint use of models of different classes together with the consideration of different aspects of the behavior of agents in cyberconflict allows to obtain a synergistic effect of the proposed modeling methodology. This approach can be considered as the closure of many conditions for the manifestation of the synergistic properties of the proposed methodology for modeling the conflict-cooperative interaction of the parties to the cyber conflict.

The second section proposes the concept of information security in social networks, based on mathematical models of information security, taking into account the specific parameters of the social network, external influences on the network, taking into account the nonlinear relationships of the parameters with the protection system and the parameters of the influence of individual characteristics of users and the nature of the relations between them.

The third section considers the practical aspects of the methodology for constructing postquantum algorithms of asymmetric McEliece and Niederreiter cryptosystems on algebraic codes (elliptical and modified elliptical codes), their mathematical models and practical algorithms. Hybrid crypto-code constructions of McEliece and Niederreiter on unprofitable codes are offered, which allow to reduce energy costs for realization considerably, thus the necessary level of cryptostability of system as a whole is provided. The concept of security of corporate information and educational systems on the basis of construction of adaptive system of information protection is offered.

The monograph will be useful for researchers and applicants for scientific degrees, and can also be used by students during training to raise awareness of information and cybersecurity issues of modern information technologies.

1 INTRODUCTION

A feature of the present time is the transition from an industrial society to an informational one. At the same time, information becomes a more important resource than material or energy resources. The rapid growth of computing resources, the emergence of a full-scale quantum computer increases the requirements for security systems not only for information and communication systems, but also for cyber-physical systems and technologies.

The main types of models used in modeling the behavior of intelligent agents are discussed in Chapter 2. The joint use of models of different classes together with the consideration of various aspects of the behavior of agents in conditions of cyber conflict makes it possible to obtain a synergistic effect of the proposed modeling methodology. The originality of the approach associated with the introduction into consideration of the concept of the contour of business processes as an integral object to be protected. Joint consideration of the contour of business processes of the organizational and technological system and the contour of business processes of the cybersecurity system can be considered as another condition for the manifestation of the synergy of the processes under consideration. Also worthy of attention is the idea of the spatio-temporal structure of the model basis proposed by the authors, which reflects not only the distribution of the set of models over the corresponding levels of the proposed methodology, but also sets the sequence of their interaction. This approach can be considered as the closure of a set of conditions for the manifestation of the synergistic properties of the proposed methodology for modeling conflict-cooperative interaction between the parties to a cyber conflict.

In Chapter 3 the concept of ensuring the protection of information in social networks is proposed, based on mathematical models of information protection, taking into account the specific parameters of the social network, external influences carried out on the network, taking into account the nonlinear relationships of the parameters with the protection system and the parameters of the impact of individual characteristics of users and the nature of connections between them.

In Chapter 4, practical aspects of the methodology for constructing post-quantum algorithms for asymmetric McEliece and Niederreiter cryptosystems on algebraic codes (elliptic and modified elliptic codes), their mathematical models and practical algorithms are considered. Hybrid crypto-code constructions of McEliece and Niederreiter on defective codes are proposed. They can significantly reduce the energy costs for implementation, while ensuring the required level of cryptographic strength of the system as a whole. The concept of security of corporate information and educational systems based on the construction of an adaptive information security system is proposed.

The material of the monograph is scientifically new and, in many respects, contains its own results of scientific research obtained by the authors and published in a number of scientific articles. The material is presented at a high scientific and, at the same time, accessible level, and is properly formatted.

2 METHODOLOGY FOR COOPERATIVE CONFLICT INTERACTION MODELING OF SECURITY SYSTEM AGENTS

ABSTRACT

The main types of models used in modeling the behavior of intelligent agents are discussed. The modeling methodology for the antagonistic agents behavior is proposed. The methodology is based on joint use of models of different classes together with the consideration of various aspects of the behavior of agents in conditions of cyber conflict. This statement makes possible to obtain a synergistic effect of the proposed modeling methodology. The originality of the approach associated with the introduction into consideration of the concept of the business processes loop as an integral object to be protected. Joint consideration of the business processes loops of the organizational and technological system and the business processes loops of the cybersecurity system can be considered as the condition for the manifestation of the synergy of the processes under consideration. The proposed approach of the spatio-temporal structure of the model basis reflects not only the distribution of the set of models over the corresponding levels, but also sets the sequence of their interaction. This approach is based on classificatory of cyber-treats for cyber-physical system.

KEYWORDS

Antagonistic agents, cyber-physical system, synergistic effect, modeling methodology, business processes loop, spatio-temporal structure.

As the world becomes more technological and dependent on computers to monitor vital functions or conduct business, the importance of ensuring the security of these systems is becoming critical in everyday life.

The most volatile aspect of a cyberattack is the attackers themselves. Modeling only a network can show its weaknesses and potential attacks that can be implemented. But this does not provide any information about what attacks can be carried out by attackers, based on their point of view. Because each person is individual, the process by which an attacker will attack the network will be different for each attacker. Understanding differences between attackers and their behavior can be used to analyze the consequences of attacks, and then for early detection and prediction.

By simulating cyberattacks, focusing on how a real cyber attacker will make decisions based on skills, rules, and knowledge, it is possible to synthesize data about an attacker's behavior that would otherwise be difficult to achieve. The combination of rule-based and knowledge-based attack generation provides reliable and diverse generations of attack trajectories, while providing realistic results because rules and knowledge are constantly coordinated with each other. This means that rules cannot be applied if knowledge is underdeveloped, and knowledge flexibility cannot be used if the rules are too limited. Applying this scheme to simulation allows a better understanding of how many different types of attackers affect by analyzing the types of attacks performed and being able to learn what the attacker needed to know to perform attacks. Finally, you should turn to potential find users trying to protect their networks from attacks that intrusion testers didn't think of, or other tools that don't have security tools. This provides a deeper understanding of how vulnerabilities are exploited and how they can affect the network before an attack can occur, and then something can be done about it. The cybersecurity industry is trying to meet today's requirements by introducing new and more advanced security technologies and methods. Modern methods of studying cyber threats are usually performed using static analysis of network and system vulnerabilities. But only a few addresses the most volatile and most important part of the problem – the attackers themselves. The human factor underlying cybersecurity provides a better understanding of this issue and highlights the behavior of individuals as a key factor of greatest concern. The human element at the heart of cybersecurity is what makes cyberspace a complex, adaptive system. A comprehensive, interdisciplinary, comprehensive approach that combines technical and behavioral elements is needed to increase cybersecurity. Therefore, the creation of a scientifically sound methodology for modeling the processes of agent behavior in security systems is an urgent scientific and applied problem of theoretical and practical significance.

2.1 THE TRADITIONAL APPROACH TO MODELING THE BEHAVIOR OF AGENTS IN SECURITY SYSTEMS

In recent years, research has been conducted on the dynamics and implementation of cyber-attacks to better analyze the impact of those attackers. Studies have been conducted on the use of network vulnerabilities to identify possible and realistic ways to attack [1–6]. Thus, [1] provides specific examples of large-scale cyber-attacks. The paper [2] analyzes the trend of using third-party service providers to gain access to victim organizations. A new paradigm of attack graph analysis, which complements the traditional graph-centric representation based on graphs adjacency matrices, is presented in [3]. The work [4] is devoted to the issue of forecasting potential attacks on the basis of observed attacks. [5] gives an example of a Bayesian network based on the current model of the security graph. The variable-length Markov model, which captures the features of attack tracks, which allows predicting the probable subsequent actions in current attacks, is analyzed in [6]. It should be noted that the disadvantage of these works is that these methods take into account only vulnerabilities in the network, but do not reveal real differences between the types of attackers. In other works, this issue was considered by modeling the capabilities of opponents [7] or applying the methodology of game theory [8] to simulate the attacker and defender. None of these methods simulate an attacker based on the information that an attacker receives during an attack, although it plays an important role in making decisions about the attack. This concept is well implemented in agent modeling methods in the NeSSi2 (NeSSi – Network Security Simulator) [9] and in the attacker's behavior model in multistage attack scenario simulation (MASS – multistage attack scenario simulation) [10]. However, agent modeling techniques do not provide a structure in which an attacker obtains specific details about targets and can dynamically change targets and strategies during an attack. This type of knowledge-based design for attacker modeling makes it possible to flexibly describe cyber-attacks, which allows modeling the proactive and reactive behavior of participants in cyber conflict.

In [10, 11], simulations were performed to analyze possible cyber-attacks that may occur in the network. The paper focuses on modeling the behavior of a cyber attacker so that it is possible to flexibly describe many different types of attackers, while maintaining reasonable realism in the types of attacks that can be performed. Modeling attacker's decision-making processes in terms of reflexive control is more like how an attacker actually thinks. This allows understanding the features that different attackers have in the same network, or how one attacker can affect different types of networks. This flexibility can help to ease the skills and to reduce the time to perform this type of analysis. The main goal is to develop a structure for modeling the attacker's decision-making process, based on both deterministic factors, such as network and knowledge, as well as probabilistic factors. This structure takes into account randomness in the simulation. Although the goal is not to be able to model each type of attacker's behavior comprehensively, but to determine what exactly needs to be modeled to describe the attacker.

Cyber threat analytics is a relatively young industry and is diverse in the types of approaches used to perform predictive cyber-attack analysis. These approaches consist of vulnerability assessment and mitigation, analytical approaches such as the use of attack graphs and game theory, and mathematical modeling and simulation of cyber-attacks. Each approach has its advantage and disadvantages, and one approach is not necessarily better than another because of the complexity of predicting, primarily human behavior. Currently, mathematical models such as attack graphs, attack ontologies or simulation, game theory models, or multi-agent models are used to analyze the enemy.

The purpose of a network intrusion test is to identify potential vulnerabilities in a network accessible to a potential attacker. Knowing the vulnerabilities of the network, the tester/attacker can use them to further penetrate the network for more information. This intrusion tester will use this information to detect more vulnerabilities until the attackers have exhausted all their option *s*. To do this, a so-called attack graph is developed, which is a set of all possible ways that an attacker can follow in the network. This process has traditionally been performed manually by an attacker or a group of analysts and can be a grueling process. In [12], the process is formalized to automatically generate a comprehensive set of possible attack graphs for a given network. Attack graphs are generated using a description of the network and the attacker's knowledge of that network. followed by a description of a set of states that describe the actual attacks that may occur. In [12], a network of two hosts with an IDS (IDS – Intrusion detection system) and a firewall was modeled. The result was an attack graph of 5,948 nodes with 68,364 edges, which is extremely large for very few types of attacks and unrealistically small network. This method of analysis is not flexible, scalable or easy to use, which is necessary to successfully assess network weaknesses.

Given the size of the network, it should be noted that the number of possible ways of attack can be extremely large. In [13], two methods were proposed to determine which attack graphs are the most critical and which are the most effective. Automatic attack graph generation requires modeling of all possible types of attacks. The paper [13] considered only 4 possible types of attacks.

The use of attack graphs to generate IDS alert templates to help predict future and ongoing attacks is described in [14]. Using these attack graphs and knowledge of the area of cyber-attacks, the probability of achieving attack goals to predict future attacks can be estimated. This method requires that each attack graph be converted to a network, and a cybersecurity expert analyze it to determine the likelihood of a successful cyber-attack. This approach has two problems: the first attacks that do not strictly follow the attack plan cannot be modeled, and the probability is based solely on the expert's experience. [13, 14] define only the different ways that an attacker can follow, and not whether the attacker will actually implement this attack or not.

In [15], the authors eliminated the uncertainty of attack variation, success and accuracy of sensory warning data by combining attack graphs with Bayesian networks. This has led to the creation of real vulnerability databases, such as the National Vulnerability Database (NVD) and the Common Vulnerability Scoring System (CVSS). Using real data from these databases provides a basis for calculating the probability without the need for expertise for each function.

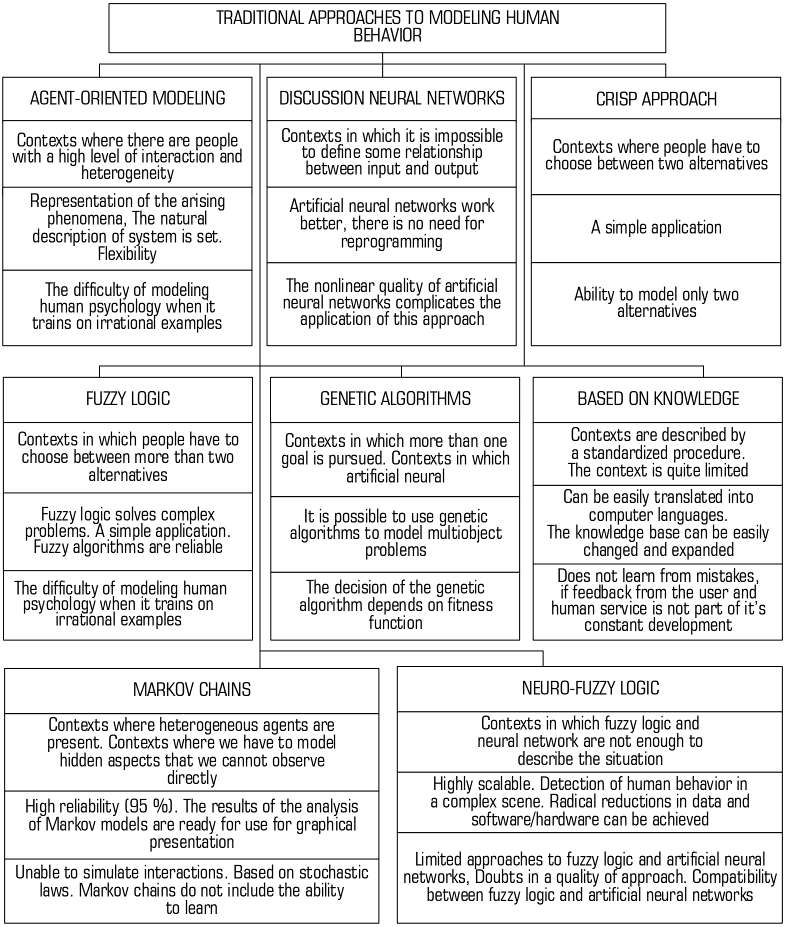
In [16, 17], the generation of a real-time attack graph is estimated to predict the probability of an attacker's next steps based on various security breaches. Based on security breaches, the basic level of attacker's skills can be determined, which can then be used with CVSS to determine the possibility of further steps based on the attacker's position in the network. A common problem of the above works is the development of a base attack graph that describes the attacker's scenario and targets. Using common attack pattern enumeration and classification (CAPEC) from MITRE, attack graphs based on real scenarios are generated in [18, 19]. These scenarios are used to obtain more realistic predictions and other attack graphs.

In [12–19], network security is analyzed on the basis of possible attacks that can be implemented in the network in one or more scenarios. In these cases, the scenarios are clearly defined, and different attackers may pursue the same goal, regardless of whether they are successful or not. Understanding the attacker's impact on a network is very important, because in fact not all vulnerabilities can be closed, and some can prioritize which vulnerabilities need to be addressed over time. Suppose there is an exploit that can be performed by anyone and that can have a harmful effect on the network. In this case, it should have a higher priority than the exploit, which only 1 % attackers can perform on a non-critical machine. Publications [15–17] show the use of publicly available data from cyber-attack scenario s to create attack paths that were identified as realistic but did not take into account the skills or behavior of the attacker. Modern cyber attack predicting methods have become more focused on the behavior and decision-making of the attacker during the attack. Publications in scientific periodicals can be divided into two categories. The first category includes publications focused on methods of modeling the behavior of interacting agents. The second includes publications, focused on the behavioral aspects of security agent *s*, and more specifically on decision-making processes. Attention to the use of game theory is due to the fact that this theory is the basis for agent modeling in conflict. **Fig. 2.1** demonstrates the results of the analysis of modern approaches to agent behavior modeling, the main advantages of which are the following:

– reflection of the purposefulness of agents' behavior, as well as the agents' ability to formulate their goals in the model;

– ability to simulate both the behavior of an individual agent and the interaction between different agents that make up the model;

– learning ability of agents.



TRADITIONAL APPROACHES TO MODELING HUMAN BEHAVIOR

AGENT-ORIENTED MODELING

Contexts where there are people with a high level of interaction and heterogeneity

Representation of the arising phenomena, The natural description of system is set. Flexibility

The difficulty of modeling human psychology when it trains on irrational examples

DISCUSSION NEURAL NETWORKS

Contexts in which it is impossible to define some relationship between input and output

Artificial neural networks work better, there is no need for reprogramming

The nonlinear quality of artificial neural networks complicates the application of this approach

CRISP APPROACH

Contexts where people have to choose between two alternatives

A simple application

Ability to model only two alternatives

FUZZY LOGIC

Contexts in which people have to choose between more than two alternatives

Fuzzy logic solves complex problems. A simple application. Fuzzy algorithms are reliable

The difficulty of modeling human psychology when it trains on irrational examples

GENETIC ALGORITHMS

Contexts in which more than one goal is pursued. Contexts in which artificial neural

It is possible to use genetic algorithms to model multiobject problems

The decision of the genetic algorithm depends on fitness function

BASED ON KNOWLEDGE

Contexts are described by a standardized procedure. The context is quite limited

Can be easily translated into computer languages. The knowledge base can be easily changed and expanded

Does not learn from mistakes, if feedback from the user and human service is not part of it's constant development

MARKOV CHAINS

Contexts where heterogeneous agents are present. Contexts where we have to model hidden aspects that we cannot observe directly

High reliability (95 %). The results of the analysis of Markov models are ready for use for graphical presentation

Unable to simulate interactions. Based on stochastic laws. Markov chains do not include the ability to learn

NEURO-FUZZY LOGIC

Contexts in which fuzzy logic and neural network are not enough to describe the situation

Highly scalable. Detection of human behavior in a complex scene. Radical reductions in data and software/hardware can be achieved

Limited approaches to fuzzy logic and artificial neural networks, Doubts in a quality of approach. Compatibility between fuzzy logic and artificial neural networks

Fig. 2.1 Traditional approaches to modeling human behavior

In [18–20], the authors propose approaches to assess the quality-of-service base d on multifactor analysis and the current state of information security of the organization. However, possible preventive actions based on modeling and evaluating the capabilities of both the attacker and the defense side are not taken into account.

Thus, the analysis of the possibilities of ensuring both the security of the business process contour and the tasks of modeling the behavior of antagonistic agents, showed the following. Along with a large number of works on the security of organization's business processes, the problem of creating a holistic modeling methodology remains unresolved.

The implementation of such a methodology in practice will contribute to the sustainable development of security systems of any level, based on modeling the behavioral characteristics of security system agents.

The lack of an appropriate methodology today is due to the contradiction, which is defined as follows. Practice requires the theory to find new approaches to cybersecurity and information security of the business process contour in terms of increasing the number of threats while increasing their technological complexity.

2.2 AGENT-BASED MODELS OF THE PARTIES TO THE CYBER CONFLICT. THE MAIN DIRECTIONS OF THE CLASSIFICATION OF METHODS OF AGENT-BASED MODELING

When developing programs to simulate agent behavior, it is necessary to answer the question of how to model the decision-making processes of agents in the security system.

In computational social science in general and in the field of agent-based social modeling (ABSM), in particular, there is a constant discussion about the best way to simulate human decision-making. The reason for this is that most computational models of the decision-making process are quite simple [21]. As with any good scientific model, when modeling human behavior, the objects being modeled should be analyzed in terms of only those properties that are relevant to the given behavior scenario.

Therefore, the question arises: «What is a good (computational) human (and decision-making) model for a particular research issue?»

A large number of architectures and models have been developed for ABSM that attempt to represent the human decision-making process. Despite the common goal, each architecture has slightly different goals and, as a result, includes different assumptions and simplifications. Therefore, knowledge of these differences is important when choosing an agent's decision model in ABSM.

To be able to discuss the suitability of different agent architectures for different types of ABSM, it is necessary to answer the questions of which types of ABSM exist and which ones are of interest to the ABSM community.

One of the previous attempts to classify ABSM was made in [22]. The paper identifies five high-level aspects by which ABSM as a whole can be classified, including the extent to which ABSM attempts to include details of specific objectives The last of these measurements concerns agents (and decision making), comparing ABSM by the complexity of the agents they model. According to Gilbert, this complexity of agents can vary from «product system architectures» (i.e. agents that follow simple IF-THEN rules) to agents with complex cognitive architectures such as SOAR (Security Orchestration, Automation and Response (symbolic cognitive architecture)) or ACT-R (Adaptive Control of Thought – Rational). Considering the suitability of different architectures for different research issues, [23] concludes that simpler agent models come in handy when the goal is to predict the behavior of the organization as a whole. Whereas accurate representations require complex and more cognitively accurate architectures to predict behavior at the level of individuals or small groups.

In [24], three categories of models are proposed:

– physical models that assume that people respond mutually to current (and/or past) interactions;

– economic models that assume that people respond to their future expectations and make decisions in a selfish way;

– sociological models that assume that people respond to their own and others' expectations (as well as to their past experiences).

In the classification [24], simple agent architectures, such as rule-based production systems, are best suited for physical models, and the complexity and capabilities of agents will need to increase in the transition to sociological models. In these sociological models, the emphasis on modeling social (human) interaction may require the agent to perceive the social network he or she is embedded in, or even the requirements for more complex social concepts.

Summing up, two main dimensions should be identified that are useful for distinguishing between agent architectures:

– cognitive level of agents, i.e. they are purely reactive or inspired psychologically or neurologically (to model person's decision-making as accurately as possible);

– social level of agents, i.e. the degree to which they are able to distinguish between social network relationships (and status), what levels of communication they are capable of, whether they have a theory of thinking or to what extent they are able to perceive complex social concepts.

Another way to classify ABSM in terms of applications is given in [25]. Examples of application areas include: emergence and collective behavior, development, learning, norms, markets, institutional design and (social) networks.

Other candidates for distinguishing agent architectures are:

– agents' ability to think about (social) norms, institutions and organizational structures; what impact norms, policies, institutions and organizational structures have on system performance at the macro level; and how to design regulatory structures that support the goals of the system developer (or other stakeholders);

– agents' ability to learn and, if so, at what level they can learn; for example, whether agents are able to learn only the best values of their decision-making functions and whether they can learn new decision-making rules.

So, two more dimensions should be added: norm and learning.

The last dimension proposed by researchers is the affective level that the agent is able to express.

Most of the categories found are similar [25]. They also include emotions as an area of research.

Summing up, five main dimensions can be identified to classify the operation of ABSM in general and, therefore, to determine the agent's architecture, which are shown in **Fig. 2.2**.

Production rule systems are symbolic systems, which consist of a set of behavioral «IF-THEN rules» [26, 27], and are an information processing architecture based on pattern matching. The main components that make up production rule systems and determine which actions are selected by the agent on the basis of input data (the so-called direct recognition cycle [28]) are shown in **Fig. 2.3**.

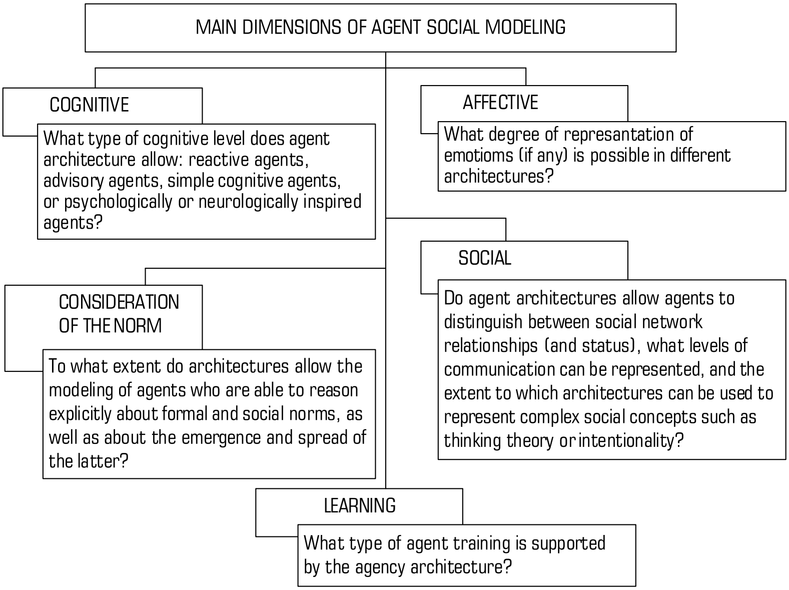

MAIN DIMENSIONS OF AGENT SOCIAL MODELING
COGNITIVE
What type of cognitive level does agent architecture allow: reactive agents, advisory agents, simple cognitive agents, or psychologically or neurologically inspired agents?
AFFECTIVE
What degree of represantation of emotioms (if any) is possible in different architectures?
SOCIAL
Do agent architectures allow agents to distinguish between social network relationships (and status), what levels of communication can be represented, and the extent to which architectures can be used to represent complex social concepts such as thinking theory or intentionality?
CONSIDERATION OF THE NORM
To what extent do architectures allow the modeling of agents who are able to reason explicitly about formal and social norms, as well as about the emergence and spread of the latter?
LEARNING
What type of agent training is supported by the agency architecture?

Fig. 2.2 Main dimensions of ABSM classification

Advantages:

– simplicity in terms of understanding the relationship between rules and their results;

– availability of convenient graphical tools for presenting decision-making processes (for example, decision trees).

Disadvantages:

– incomplete adequacy for modeling human behavior;

– agents of production rule systems are generally incapable of affective behavior, understanding and responding to norms, considering social structures (including communication), or learning new rules or updating existing ones;

– ability to model the agent's behavior only due to the great complexity and use of many rules;

– increase the likelihood of conflicts between the rules as their number increases;

– long computing time under a large number of decision-making rules.

The Belief-Desire-Intention (BDI) and emotional BDI (eBDI) models are one of the most popular models for agent decision-making in the agent environment. The model is especially popular for building reasoning systems for complex problems in dynamic environments [29].

In contrast to the production rule system, the basic idea of BDI (Belief-Desire-Intention) is that agents' mental state is the basis for their reasoning. As the name implies, the

BDI model is centered around three mental attitudes, namely beliefs, desires, and especially intentions [30, 31].

Table 2.1 shows the advantages and disadvantages of the BDI model depending on the purpose (modeling) [32–35].

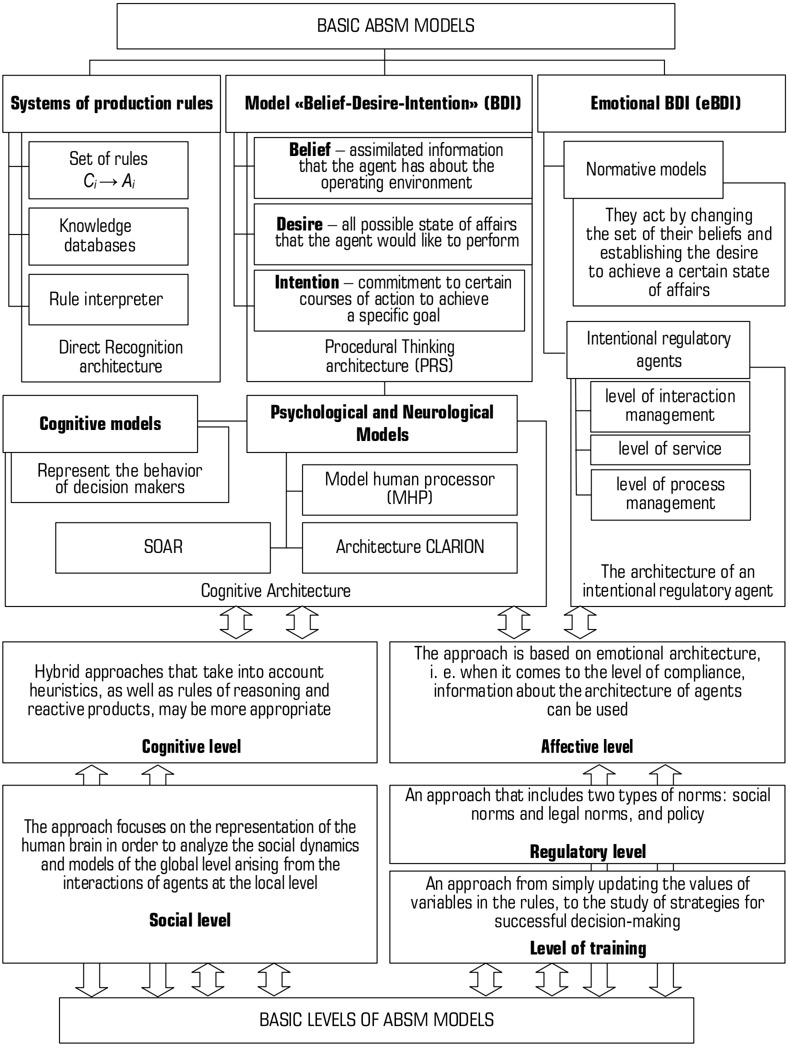

BASIC ABSM MODELS
Systems of production rules
Model «Belief-Desire-Intention» (BDI)
Emotional BDI (eBDI)
Set of rules $C_i \rightarrow A_i$
Knowledge databases
Rule interpreter
Direct Recognition architecture
Belief – assimilated information that the agent has about the operating environment
Desire – all possible state of affairs that the agent would like to perform
Intention – commitment to certain courses of action to achieve a specific goal
Procedural Thinking architecture (PRS)
Normative models
They act by changing the set of their beliefs and establishing the desire to achieve a certain state of affairs
Intentional regulatory agents
level of interaction management
level of service
level of process management
The architecture of an intentional regulatory agent
Cognitive models
Represent the behavior of decision makers
Psychological and Neurological Models
Model human processor (MHP)
SOAR
Architecture CLARION
Cognitive Architecture
Hybrid approaches that take into account heuristics, as well as rules of reasoning and reactive products, may be more appropriate
Cognitive level
The approach is based on emotional architecture, i. e. when it comes to the level of compliance, information about the architecture of agents can be used
Affective level
The approach focuses on the representation of the human brain in order to analyze the social dynamics and models of the global level arising from the interactions of agents at the local level
Social level
An approach that includes two types of norms: social norms and legal norms, and policy
Regulatory level
An approach from simply updating the values of variables in the rules, to the study of strategies for successful decision-making
Level of training
BASIC LEVELS OF ABSM MODELS

Fig. 2.3 Shows the basic ABSM architectures, relevant models and application levels

⬢ **Table 2.1** Advantages and disadvantages of the BDI model depending on the purpose

Purpose of modeling	**Importance of BDI**	**Advantages**	**Disadvantages**
Forecasting	Average	Realism, adaptable to behavior at the micro level, possibly irrational individual cognition	Complexity, scalability Detailed data is required
Task execution	High	Correct level of human behavior abstraction Awareness, cooperation in mixed human-agent teams Modular, scalable, flexible design	More complex design, unusual paradigm
Training	High	Accurate realistic behavior for better immersion in the game. Adaptability to a dynamic environment. Descriptiveness	More complex design, unusual paradigm
Using game theory	Average	Plausible human behavior: immersion, challenge Quick solution in case of uncertainty and incomplete information Correct level of abstraction to display real player strategies	Scalability, performance More complex design compared to scenarios
Education	Average	Intuitive explanation of behavior using built-in concepts of psychology (*B*, *D*, *I*)	Unnecessary realism and complexity for non-essential agents
Evidence	Low	Realistic knowledge needed to prove micro-, macro-connections and complex socio-cognitive phenomena	Realism and complexity are not needed to prove a simpler hypothesis
Revelation	Low	Realistic detailed behavior model for detecting unintuitive effects and micro-, macroconnections in adaptive dynamic complex systems	More complex understanding and deduction More complex specification of decision rules

Normative models [36]. In BDI, agents act by changing a set of beliefs and establishing a desire to achieve a certain state of affairs (for which agents then choose specific intentions in the form of plans they want to carry out). Agents' behavior is driven solely by their intrinsic motivators, such as beliefs and desires. The advantage of normative models was the use of an additional element that influenced the agent's reasoning. Unlike beliefs and desires, this element was external to the agent, and it took into account the behavioral norms established in the environment in which the agent was. Therefore, such elements were considered as external motivators, and agents in the system were called agents regulated by the relevant norms.

Intentional normative agents focus on the idea that social norms should be involved in the agent's decision-making process [37]. That is, autonomous agents should be able to reason, communicate, and negotiate norms, including deciding whether to violate social norms if they are unfavorable to commercial agents.

The advantages of this model are:

– ability to represent social norms not just as constraints and external fixed rules in the agent architecture [38], but also as mental objects. These objects have their own mental representation and interact with other mental objects (i.e. beliefs and desires) and the agent's plans [39];

– allocation of separate levels of the agent architecture. The first level is the interaction management level, which controls the agent's interaction with other agents (through communication), as well as the overall environment. The second level is the information service level, which stores the agent's information about the environment (information about the world), about other agents and about the agent society as a whole. The third level includes the process management level, where information is processed and decisions are justified. This allows, on the one hand, considering the relevant processes as relatively independent, and on the other – as different manifestations of one general process of agent behavior;

– ability to display semantic differences between different types of information (three levels of information: one object level and two metalevels). The object level includes information that the agent believes in. The first metalevel contains information on how to process input information based on its context. Meta-information determines how an agent's internal processes can be changed and under what circumstances.

The disadvantages are as follows:

– emergence of an additional level of complexity due to the fact that the norms learned by the agent can affect both the generation and the choice of intentions.

Cognitive models [40] and social modeling models, although they often pursue the same goal (represent the behavior of decision-makers), tend to have a different idea of what is a good model for human decision-making.

As a disadvantage, it is noted that social modeling researchers often focus only on agent models specially adapted to the task, which limits the realism and applicability of social modeling.

The advantages of this class of models are clearly manifested in the form of the results of cognitive processes, namely the construction of so-called cognitive maps:

– clarity of factors influencing the decision-making process;

– clarity of connections between factors (not only qualitative, but also quantitative);

– ability to conduct so-called cognitive modeling, changing the weight of a factor that affects the final decision.

Psychological and neurological models are often referred to as cognitive architectures. However, because they have a different focus than the «cognitive architectures» that were mentioned, they are allocated to a separate group. The mam difference and advantage is that their architectures take into account the expected structural properties of the human brain.

Model human processor (MHP) [41, 42] is based on the synthesis of cognitive science and human-computer interaction. The advantage of the Model Human Processor is that if includes detailed specifications of the duration of actions and cognitive processing and breaks down complex actions into detailed small steps that can be analyzed. This allows system developers to predict the time it takes for a person to complete a task, avoiding the need to experiment with the people involved.

The advantages of the CLARION [43] architecture are as follows:

– use of hybrid neural networks for modeling problems in cognitive and social psychology, as well as for implementing intelligent artificial intelligence systems. This makes it relatively easy to implement architectures of this class on any artificial neural network platforms;

– presence of a built-in motivational structure and meta- cognitive structures;

– presence of two dichotomies: explicit and implicit representation, focused on action rather than representation;

– combining training from top to bottom and from bottom to top;

– inclusion of a number of functional subsystems that significantly expand both the scope of the architecture and the set of processes to be modeled. The main of these subsystems are as follows. The action-oriented subsystem that controls all actions. The action base subsystem supports knowledge, both explicit and implicit. The motivational subsystem provides the main motivation for perception, action and cognition. The metacognitive subsystem dynamically monitors and manages the operations of all subsystems.

Thus, the CLARION architecture combines reactive procedures, general rules, training and decision-making to develop universal agents that learn under specific conditions and summarize the knowledge gained in different environments.

SOAR [44] is a symbolic cognitive architecture that implements decision-making as purposeful behavior, which includes searching in the problem space and studying the results.

The advantages of this architecture:

– consideration of decision-making processes as a combination of search in the problem space, and study of the obtained results (i.e. feedback systems);

– combination of results of studying human behavior (descriptive models) and results of artificial intelligence (prescriptive models);

– use of two memory types in the system architecture: symbolic long-term memory (production rules), and short-term (working) memory (graph structure to allow the representation of objects with properties and relationships);

– ability to apply the rules in parallel, extracting several pieces of knowledge simultaneously;

– availability of additional context-sensitive knowledge for the decision-making process;

– distribution of operators according to several rules, which allows flexible presentation of knowledge about operators, as well as constant updating of knowledge structures for operators, allowing to redefine operators if required by circumstances.

These models can be used at different levels of application, as shown in **Fig. 2.3**.

2.3 GAME-THEORETIC MODELS OF CONFLICT SITUATIONS

Networks have become a traditional tool in people's lives, users are very dependent on networks to provide comfortable communication and convenient access to information. Modern information and communication technologies are developing rapidly, not only in terms of complexity, but also in terms of their diversity. The growing complexity, ubiquity and connectivity of modern information systems pose new challenges in the field of security, and cyberspace has become a platform for people with different levels of skills and all kinds of intentions (both positive and negative). Thanks to round-the-clock communication, which has become an integral part of people's daily lives, the protection of information, personal data and assets has become even more important than ever. Traditional security has come a long way towards protecting clearly defined goals, such as confidentiality, integrity, accessibility and authenticity (CIA$^+$).

Along with the expansion of the scope of services provided by network services, the problems associated with the safe use of network services are growing. Network security is becoming a complex topic, as many new network attacks, which are becoming hybrid, are becoming more sophisticated and lead to huge losses of network resources. A crime area such as cybercrime has formed, which requires the closest attention due to the prevalence of the computer as a tool in various areas of human activity. Like other forms of crime, the causes of cybercrime are difficult to determine, however, as a rule, this is due to some factors, which include high financial gain, personal emotions and even revenge, as well as ethical, ideological, moral and environmental problems.

Most cybersecurity studies focus on either presenting a specific vulnerability or proposing a specific defense algorithm against a well-defined attack pattern. Although such cybersecurity research is important, attention should be paid to the dynamic interaction between attackers and defenders, where both sides are intelligent and can dynamically change their attack or defense strategies to defeat their opponents. This phenomenon of «cyber warfare's exists in most cases of cybersecurity in the real world» [45].

It is necessary to emphasize the following. On the one hand, the weakness of traditional solutions for network security lies in their lack of a system of quantitative solutions [46].

On the other hand, security assessment [47] is an important aspect of network security; this is an assessment of confidentiality, integrity, availability, vulnerability and security risks. Network Security Measurement is a large category that includes the measurement of every aspect of network security. Risk assessment [48] is one such measure. Network security measurements include interactions between attackers and defenders, and their interactions can influence the measurement result. One of the metrics in assessing the risk for a network system is the probability of its attack. It is necessary to predict the actions of both defenders and attackers.

To solve the problems of network security, solutions based on game theory are quite often proposed, since the interaction process between attackers and defenders is considered as a game. In this case, game theory can be used in every possible scenario to predict the actions of attackers, and then to determine the decisions of defenders.

Game theory-based approaches outperform traditional cybersecurity and network privacy solutions in many ways, including the following:

– mathematical validity and provability. Most of the traditional security solutions that are implemented either in prevention devices (for example, firewalls) or in the means of rapid response to threats (for example, antivirus programs) rely only on heuristics. Nevertheless, game theory can investigate security solutions with mathematically grounded methods, the correctness and effectiveness of which can be justified mathematically;

– reliable protection. Based on the analytical results of applying game theory methods, reliable mechanisms can be developed to protect cyber systems from selfish behavior (insider or external attacks) by malicious users/nodes;

– timely response. Although the adoption of a traditional security decision is rather slow due to the lack of incentives for participants, game-theoretic approaches defend the interests of defenders using basic incentive mechanisms in the context of allocating limited resources to balance perceived risks;

– distributed solutions. Most traditional defense mechanisms make decisions centrally, rather than individually (or distributed). In network security games, a centralized approach is almost impossible because of the lack of a coordinator in an autonomous system. Using appropriate game theory models, security solutions will be implemented in a distributed manner.

These reasons favor the use of the game theory paradigm for modeling and analyzing the behavior of security systems antagonistic agents.

Game-theoretic analysis focuses on identifying the likely behavior of players with respect to the choice of strategy, thus determining the intended outcome of the game. It was noted in [49] that models based on game theory demonstrate advantages in productivity and cost compared to other risk management models associated with cybercrime. However, this does not take into account that in game theory, players are rarely completely rational and do not have complete information about each other's wins and strategies. The reason for this is either the fundamental impossibility of obtaining complete information, or the significant cost of obtaining it. In addition, limited rationality is an inherent characteristic of an agent (in contrast to the ideal player in theory). And besides, game theory has always imposed restrictions, which are the only way to correctly formulate the problem, and it is based on the assumption that the parties are rational, there are few of them and each player knows the goals of his opponent [50, 51].

One way to overcome the discrepancy in the rationality of the abstract player and the real agent of cyber conflict is defense games. Defense games study the interaction between attackers and defenders, which serve as the basis for making formal decisions and developing algorithms, as well as for predicting the behavior of attackers. The applicability of game theory in this case is due to the fact that it is a mathematical toolbox independent of the field of application, which can be used in any situation of interactive decision-making [52], for example, in computer and communication networks for modeling various problems. This approach includes work on modeling service disciplines [53], for TCP performance [54], and for modeling power control in a wireless communication system [55]. [56] described the application of game theory to develop protection against «denial of services» (DoS) attacks. In the field of MANET [57], cooperative and non-cooperative game-theoretic constructions were used to develop based on the reputation of the collaboration architecture.

The approach to the application of game theory related to the modeling of intrusion detection processes in computer systems should be noted. The authors of [58] used a game-theoretic structure to model intrusion detection using sampling in communication networks, and also developed sampling schemes that are optimal [59].

In general, the game-theoretic approach works with at least two players. The success of a player in choosing depends on the choice of others. In game theory, players clash with each other in turn to maximize their winnings in an attempt to achieve their ultimate goal [60]. In the area of cybersecurity, game theory has been used to determine the nature of cyber conflict. The attacker's decision-making strategies are closely related to the defender's strategies and vice versa.

Cybersecurity is then modeled by at least two intelligent agents interacting in an attempt to maximize their intended goals. It should be noted that this work limits the number of players to 2, suggesting the alternation of each other's moves. In real situations of cyber confrontation, this can significantly narrow the scope of game-theoretic methods.

Going beyond the limitations inherent in this work can be considered in the works [61, 62]. It was noted in the works that the various methods available in game theory can be used for tactical analysis of cyber threat options created by both one attacker and an organized group. A key concept in game theory is the ability to explore the vast number of possible threat scenarios in a cyber system. Game theory can also provide methods for proposing several possible actions along with a predicted outcome for controlling future threats. Computers can analyze all combinations and permutations to find exceptions in general rules, unlike people who tend to overlook some possibilities. This approach allows to identify what, if scenarios that the human analyst may have overlooked.

In [63, 64], the interaction between the attacker and the network administrator is presented as a game, the modeling of which allows one to determine many strategies that lead to Nash equilibrium.

In [65], a methodology was presented for modeling the interaction between an attacking DDoS and a network administrator. This approach has shown that the ability to model and identify the intentions, objectives, and strategies of an attacker (AIOS) is important because it can lead to effective risk assessment and prediction of harm. In this paper, a stimulus-based game model for outputting AIOS was discussed. Several bandwidth parameters were used as a metric to measure the effects of attack and countermeasures, which, in turn, measures the attacker's and defender's stimulus. It was also noted in the work that the best game model to be selected depends on the degree of accuracy of the intrusion detection systems (IDS) used and the degree of correlation between the stages of the attack. The topology considered in the simulation experiment consists of 64 source hosts connected to one victim machine through 4 levels of routers. Each router is able to use a reflection mechanism as part of a security strategy.

In the model presented in [64], an attacker and a network administrator participate in a two-person stochastic zero-sum game. In this work, it was assumed that the network consists of a set of interdependent nodes whose security assets and vulnerabilities are interrelated. The concept of linear influence networks was used in the work and the interdependence between nodes was modeled using two weighted oriented graphs, one of which denoted the relationship of security assets, and the other denoted a correlation of vulnerability between nodes. The numerical example presented in the paper describes a small network of three nodes and explains the method of calculating the optimal strategies of players. However, there are no mechanisms for implementing the strategies found.

In [65], an extension of traditional approaches to the use of game theory is proposed. It addresses the issue of network security as a sequence of non-zero sum games played by an attacker and defender. This game model, called «fictitious game (FG)», assumes that players cannot accurately observe each other's previous actions. In this paper, we studied the influence of error probabilities associated with a sensory system on Nash equilibrium strategies for players, taking into account two scenarios:

– each player knows about these error probabilities;

– none of the players know these error probabilities.

Both classic and stochastic FP games are investigated using simulation.

A promising approach related to the introduction of dynamics and taking into account the time characteristics of the game is presented in [66]. The paper presents a game-theoretic model of developing a response to an attack on an Internet worm. The basic idea is that defenders can choose how to organize resistance and minimize the speed of the worm. An attacker can choose the optimal distribution of the scan group to maximize the speed of infection. Thus, the game will be played between the attacker and the defender. The attacker must choose the maximum speed of the worm, while the defender wants to minimize it. If we formulate the problem in this way, then it will be a game with a zero sum and a minimax problem. The optimal solution to this problem is when the defender must deploy the application evenly across the entire IP address space or in every corporate network, so the best strategy that the attacker uses is equivalent to the random scanning strategy. This work demonstrates the application of game theory for designing the locations of vulnerable and valuable hosts on the network, which should be considered a promising area of research.

Another example of the application of game theory, which takes into account the dynamic characteristics of the game, is [67]. It presents a model for assessing the likelihood of successful attacks on a network of interdependent files and services. This paper presents a logical model that takes into account the time required to attack, crash, or repair network systems. To demonstrate the use of the game theory model, the paper gives time and topology constraints to determine if an attack or defense will succeed. The presented example describes the configuration of a high-performance web server with interdependent elements and considers the strategic actions of both the attacker and the defender.

The economic aspects of game theory in relation to security are well presented in scientific publications, given the fact that game theory was initially oriented toward economics. In [68], the problem of information security in a mobile electronic commerce network is analyzed. It is argued that the application of game theory in the field of information security is based on the hypothesis of perfect player rationality, while in reality the bulk of information security is determined by limited rationality, which is an assumption of the evolutionary game theory. The penalty parameter is introduced into the task as a parameter, which is assigned if the organization in the mobile electronic commerce network does not invest in information security. The results of modeling the dynamics of this game made it possible to obtain the return-on-investment results. This can be seen as an application of evolutionary game theory to an investment strategy in network security for maximum return. It should be noted that evolutionary games are not sufficiently used in modeling cybersecurity problems.

In [69] game theory is presented in the unusual context of analyzing a proposal for an advocate organization to invest in information security. The work is focused more on information security management than on information security technologies. The paper formulates the problem of two organizations investing in security, with parameters such as investment, security and disaster risk. Based on the payout matrix, a penalty parameter has been introduced related to the refusal to invest, which ensures the rationality of investment. In conclusion, an argument is put forward in favor of encouraging organizations to invest in information security.

A taxonomy of the application of game theory in cybersecurity, consisting of four dimensions, which provide a holistic classification covering network and computer attacks, help to improve computer and network security, and language consistency with the description of the attack, was proposed in [70]. The first dimension is the attack vector, which is used to classify an attack into an attack class. The second dimension allows to classify attacks by specific targets (for example, OS: Linux: RedHat6.0). The third dimension consists of vulnerability classification and attack usage (for example, CVE/CERT). The fourth and final dimension highlight potential payloads or related effects (such as file deletion). Each dimension provides different levels of information to successfully classify and provide attack details.

A review of publications on the application of game theory in cybersecurity demonstrated the following. Almost all publications are devoted to the development of specific models for solving specific problems, emphasizing the advantages of game theory for solving problems of this class. The scope of the game theory methodology is extensive, given the fact that the classical game theory is independent of the subject area of research and applications. Not all studies analyze the applicability of the game-theoretic modeling methodology. Under these conditions, two fundamental issues are practically not addressed. The first is related to the formulation of the limitations of the game theory methodology for solving cybersecurity problems, which has its own characteristics and can set requirements for the proposed approaches and methods. The second question logically follows from the first. In the case of improper use or fundamentally impossibility to use the methodology of game theory, which methodology should be applied taking into account the features of the tasks being solved. In other words, an approach should be proposed to evaluate and select the most appropriate methodology for modeling the behavior of security systems antagonistic agents. The questions formulated determined the relevance of this study.

We introduce the basic definitions of the basic concepts used in security tasks based on game theory (**Table 2.2**).

Based on the introduced definitions, we consider the mathematical foundations of conflict modeling and cooperation based on game theory. Suppose that the players are rational in their behavior, which implies their motivation in order to optimize the receipt of benefits based on the utility function.

The game follows certain rules according to which players can choose and implement a strategy from a set of different behavioral options in order to optimize the possible outcome of the game.

Formally, the game is described with n players with strategic spaces S_i and their payoff functions U_j respectively for each player i ($1<i<n$):

$$G=\left\{n; S_1,S_2,\ldots,S_n; U_1,U_2,\ldots,U_n\right\}. \tag{2.1}$$

The main features of game-theoretic approaches to modeling the behavior of cybersecurity systems agents are:

– restriction of strategies when releasing games;

– simultaneous moves of players in the behavior patterns of security agents;

– players' time uncertainty;

– the uncertainty in the final goal of the enemy;

– unpredictability of further player moves;

– lack of players' assessment of enemy resources, as well as its ultimate goals;

– impossibility of timely assessment of the current state of the game.

Table 2.2 Basic definitions of the game theory concepts

No.	Term	Definition
1	Game	A simplified formalized model of a real conflict situation of confronting the antagonistic parties of cyber conflict (defense and attack parties) with opposing interests that each side tries to satisfy using one or another strategy of actions, and in which it is impossible to come to an agreement satisfying both parties regarding the system administrator information resource
2	Player	The main character in the game who makes choices and takes action. A player may be represented by a person, ma- chine, or group of people in a game. In security systems, the players are the parties to the attack (attacker) and defense (system administrator)
3	Action	An action is a move in a given game
4	Payment	Positive or negative reward for the player for this action in the game. For the system administrator, this may be the cost of the purchase and installation of protective equipment and programs against each of the threats that must be minimized. For an attacker, this could be a reward for damaging the adversary
5	Strategy	The action plan (behavior scenario) in the game, which the player can implement during the game. So, for the defense side, the strategy may be «Wait and See», and for the side of the attack, «the weakest link»
6	Game with full information	A game in which each player knows the moves of all other players that are already made. A game in which the player does not know the opponent's moves is called a game with incomplete information. Cyber conflict as a game is fundamentally a game with incomplete information
7	Bayesian game	A game in which information about strategies and payouts for other players is incomplete, and the player assigns a «type» to other players at the beginning of the game. Such games are called Bayesian games because of the use of Bayesian analysis in predicting the result, which may be characteristic of modeling the reflective behavior of one side or another in cyber conflict
8	Static/Strategic Game	A one-step game in which each player chooses his own action plan and decisions of all players are made simultaneously. This means that when choosing an action plan, one side of the conflict (defense or attack side) does not obtain any information about the action plan of the opposite side
9	Dynamic game	A game with more than one stage, at each of which players can review their actions. This can be seen as a consistent structure of the decision-making problems faced by players in a static game. Game sequences can be either finite or infinite. Dynamic games are a good reflection of the behavior of players in the implementation of the attack tree
10	Stochastic game	A game that includes probabilistic transitions through several states of the system. The game starts from the initial state; players select actions and receive a reward, which depends on the current state of the game, and then the game goes into a new state with probability based on the actions of the players and the current state. It can be used in the parties' assessment of the opposition of the probabilities of a multi-step attack and methods of counteracting it

The game is presented in a strategic/expanded form that describes the actions of the players. The strategic form of the game is formalized as follows:

$$Game = \left(P, \left(S_j\right)_{j \in P}, \left(u_j\right)_{j \in P}\right). \tag{2.2}$$

There are many players P in the game. The player i can choose the strategy from S_j, and U_j – this is the player's i gain/utility. The combination of the player's selected strategies is the strategy profile, and the mixed strategy is generated from a set of pure strategies. Win function U_j represents the relationship between the input space of all possible profiles and the output space of real numbers R.

Game-theoretic analysis focuses on identifying the likely behavior of players with respect to the choice of strategy, thus determining the intended outcome of the game. This point of view on the methods of game theory determines the spectrum of directions for their application in the field of cybersecurity.

Various types of games are used to study the actions of the defender and the attacker and to simulate the interaction between them. **Table 2.3** presents game-theoretic models, security/privacy issues, and key solutions derived from the respective models.

Table 2.3 Set of game-theoretic approaches

Game model	Security problems	Solution
Static Prisoners Dilemma Game	Selfish behavior of agents on the network [28, 29], privacy on mobile social networks [30]	Nash Equilibrium
Zero-sum static game	Jamming and listening [31], denial of service attacks [32], trojans [33]	Nash Equilibrium
Stackelberg game	Cyberphysical security [36], data integrity and availability [37]	Stackelberg equilibrium
Coalition game	Selfishness in packet forwarding [36], listening [37]	Coalition Formation Algorithm
Zero-sum stochastic game	Cyberphysical Security [38], Secure Routing [39], Steganography [40]	Equilibrium (saddle point), Nash equilibrium
Bayesian game	Privacy trajectory [40], denial of service attack [41], survivability [42]	Bayes Nash equilibrium
Dynamic game	Secure Routing [43], Cyberphysical Security [38]	Saddle point (equilibrium)
Recurring game	Selfishness in packet forwarding [43]	Belief Based Strategy
Markov game	Intrusion Detection System (IDS) configuration [44], Smart-grid infrastructure protection [45], trust issue in an online social network [39]	Markov equilibrium
Evolution game	Selfishness in special networks [46], trust in autonomous multi-user networks [47]	Evolutionarily Sustainable Strategy (ESS)

In game theory, players are rarely completely rational and do not have complete information about each other's wins and strategies. Therefore, modeling the decision-making process using several equations and parameters is doubtful. There is also the difficulty of quantifying value added through cybersecurity. Lack of quantification affects the decision-making process regarding security investments. Consequently, the attitude towards security varies depending on the economic situation. This shows that the quantitative assessment of security-related concepts, such as trust, confidentiality and risk, in game-theoretic models is not an inherent property and requires additional development. Game theory also imposes restrictions, which are the only way to correctly formulate the problem, and it is based on the assumption that the parties are rational and few in number, and that each player knows the goals of his opponent.

The problems of game theory in terms of cybersecurity risk management are further exacerbated by the following aspects. The difficulty of defining an equilibrium strategy and the difficulty of quantifying security parameters (such as risk, confidentiality, and trust), choosing the appropriate game model for a given security problem, and reaching consensus on how to interpret a mixed strategy.

The interaction between attackers and defenders is the basis for making formal decisions and developing algorithms, as well as for predicting the behavior of attackers. The applicability of game theory in this case is due to the fact that it is a mathematical toolbox independent of the field of application, which can be used in any situation of interactive decision-making.

Based on the analysis, the main models of game theory are presented that provide the possibility of their application to provide basic security services.

To model the interaction in the network, several game-theoretic approaches are used, such as approaches with perfect and imperfect monitoring. In a game with imperfect monitoring, player actions may not be directly observed due to noise. On the other hand, a game is considered as a game with perfect monitoring if all players know a series of past actions and the actions of other players can be observed without interference. A static game is classified as a game with imperfect information, because each participant chooses only his own strategy.

Table 2.4 shows the main factors of the game for exchanging message packets in the network.

Thus, to provide basic security services based on the analysis of **Table 2.4** in game-theoretic models of cybersecurity systems, it is necessary to remove the limitations of the classical representation of game theory models:

– defender is always able to detect attacks;

– state transition probabilities are fixed before the start of the game, and these probabilities can be calculated from domain knowledge and past statistics;

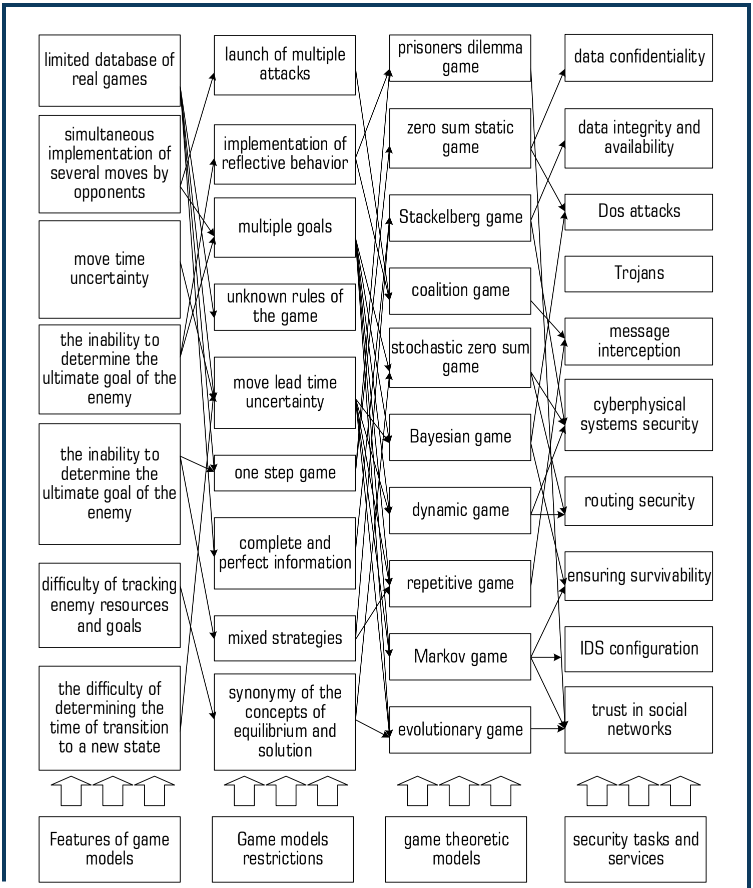
– player actions are synchronous, which is not always realistic;

– most models are not scalable due to the size and complexity of the system in question.

Table 2.4 Game theory methods for providing security services

Game model	Application area	Simulation result	Security services
Zero-sum stochastic game	Integration of a robust physical space controller	The iteration algorithm of the value to obtain equilibrium (saddle point)	Integrity, Confidentiality, Availability
Static games	Physical and cyberspace integrated using payoff function	Nash equilibrium and Stackelberg equilibrium	Integrity, Confidentiality
Dynamic games	Discrete time LTI jamming problem	Equilibrium (saddle point of the payment matrix)	Integrity, Confidentiality, Authenticity
Markov games with zero sum	Players select actions that can trigger Smart Grid system state transitions	Nash equilibrium (also a Pareto optimal solution)	Confidentiality, Integrity, Accessibility, Authenticity, Involvement
Markov game	Determination of the optimal response of the defender in a cyber-physical environment	The iteration algorithm of the value to obtain the equilibrium (saddle) point	Confidentiality, Integrity

This approach significantly affects the use of game-theoretic models and the formation of the basic principles of modeling cybersecurity systems to obtain a synergistic effect from the defender. The analysis of the use of game-theoretic modeling of the behavior of agents of security systems, the principles of building models and their limitations makes it possible to increase the security level of cyber systems based on the existing restrictions and analysis results (**Table 2.4**). **Fig. 2.4** shows a synergistic approach to the use of game-theoretic modelling taking into account the particular behavior of security system agents.


limited database of real games
simultaneous implementation of several moves by opponents
move time uncertainty
the inability to determine the ultimate goal of the enemy
the inability to determine the ultimate goal of the enemy
difficulty of tracking enemy resources and goals
the difficulty of determining the time of transition to a new state
launch of multiple attacks
implementation of reflective behavior
multiple goals
unknown rules of the game
move lead time uncertainty
one step game
complete and perfect information
mixed strategies
synonymy of the concepts of equilibrium and solution
prisoners dilemma game
zero sum static game
Stackelberg game
coalition game
stochastic zero sum game
Bayesian game
dynamic game
repetitive game
Markov game
evolutionary game
data confidentiality
data integrity and availability
Dos attacks
Trojans
message interception
cyberphysical systems security
routing security
ensuring survivability
IDS configuration
trust in social networks
Features of game models
Game models restrictions
game theoretic models
security tasks and services

⬡ **Fig. 2.4** Synergetic approach of game-theoretic modeling

Analysis of **Fig. 2.4** defines goals, objectives, and areas of application of game-theoretic modeling of the security system agent's behavior. These goals are determined by the tasks and areas of application of the considered methods (the last column of **Fig. 2.4**). The application of game theory methods allows you the selection of appropriate attack and defense strategies based on typical threats of the KDD99 technique [71], In general, the solution of these tasks provides the required level of security.

Game-theoretic models allow you to create many relevant tasks to provide basic security services: confidentiality, integrity, accessibility, authenticity. Thus, the same model can provide the solution to several security tasks, and vice versa, the same problem can be solved using different models. Because of this, in practice, it is necessary to determine the necessary subset of game models that support the solution of the entire set of security tasks, or a selected subset of them.

The choice of appropriate models will be determined by the restriction's characteristic to certain game models. The main limitations of the classical models of game theory follow from basic assumptions, namely the assumption of definiteness of the ultimate goal of the game, the synonymy of the concepts of «solving the game» and «balance», the awareness of the players about the opponent's resources, the ability of the players to construct a payment matrix, as well as the assumption of a clearly fixed sequence of players' steps that are not dependent on time. The sets of game models presented in **Fig. 2.4** are characterized by the reflection of certain restrictions in the model, which dictates their choice for solving security problems.

These restrictions follow from the features of game models that describe the behavior of players, namely, the ability of a player to detect attacks, a predetermined sequence of moves for each of the players, the probability of behavior change for games with mixed strategies, the lack of scalability of the model in size and the complexity of the task for certain game-theoretic models.

This approach significantly affects the use of game-theoretic models and the formation of the basic principles of modeling cybersecurity systems to obtain a synergistic effect from the defender.

Analysis of **Fig. 2.4** allows to conclude that the advantages of using game theory in the field of cybersecurity cannot always be realized due to differences between the real field of cybersecurity and traditional game domains. A significant obstacle to the use of game-theoretic modeling of the processes of behavior of antagonistic agents of security systems is the set of limitations organically inherent in game theory.

Thus, in real conditions, there are many characteristics that contradict the simple implementation of standard search methods.

Game theory allows to determine the optimal strategy, but does not give any recommendations regarding the implementation of this strategy. The list of standard terms used in game theory does not include the term «behavior». In other words, game theory works more at the strategic level, not dropping to the operational level. Due to this, it does not take into account the peculiarities of behavior and the real characteristics of the players. Therefore, to model the behavior, reflect the reflective characteristics of the players and deviate from the principle of rationality in making decisions, different approaches from game theory should be used. Game theory models can be used to solve particular problems of behavior modeling without claiming the status of the main modeling methods. This situation confirms the thesis that the breadth of the problem is achieved, most likely, by increasing the level of abstraction and moving away from taking into account the characteristics of real players, their behavior, goals and methods of achieving them.

The revealed limitations inherent in the game-theoretic methodology for modeling the behavior of agents of security systems emphasize the fact that this methodology is not universal, although it has a wide scope. The consequence of this is the need to compare the specified methodology with other methodologies used for the indicated purposes.

The choice of a particular methodology should be based on a comparison of the most common modeling methodologies.

Thus, it is proposed to conduct a comparison according to the following criteria:

– the time and effort required to apply the methodology of modeling and designing the current model with the participation of future users;

– user requirements. The amount of technical knowledge and the level of training necessary for the user to understand and use the model;

– studying time. Time and effort for a typical user to study the designed model and the rules for its use;

– model flexibility. The simplicity with which a developer can change the model to include a new variable or change the variables used;

– number of existing analog models with functions that can be adapted to be used as part of the behavior model of security agents;

– transparency. The simplicity with which the user can discover in the model everything that can affect the simulation results.

2.4 SYSTEM-DYNAMIC MODELS OF CONFLICT-COOPERATIVE INTERACTION OF AGENTS

When developing a model of behavior, it is first necessary to determine the boundary of applicability of the model and the main assumptions included in it. The proposed model focuses on the dynamics of the interaction of the attacker and the defender in the field of information security to determine the investment strategies used by opponents.

The model represents the company as a defender, which protects the asset from a group of attackers who are trying to violate the security of the company's asset with the help of malicious cyber-attacks. An asset can take many forms, such as a customer list, website, payables register, or strategic plan. Increased security may be associated with protecting the confidentiality, integrity, authenticity or availability of the asset for authorized users.

Modeling is limited to three possible threat vectors. Protection against each of the threat vectors is realized as a result of investing in appropriate protection. Defense is considered effective if it can compensate for incoming attacks.

The list of basic concepts and concepts underlying the developed model, which underlie the interaction of the defender and the attacker in a dynamic behavior model, includes the following [72].

Reputation of the company – a profitable and universally recognized name for merits, achievements, reliability, etc. In this case, the reputation refers to the public authority of the company.

Vulnerability is the level of security possessed by company assets. It can also be called an asset protection level.

Security vectors are externally visible and accessible system resources that can be used to organize attacks on the system. The weight (or magnitude) of the vector is specified in accordance with the potential damage that could be caused by any exploitation of the vulnerability.

Examples of security vectors are: network servers, web pages, email, mobile devices, system configuration, and others.

Opportunities of defenders – available resources of defenders, which are distributed between security vectors to increase the level of protection of assets.

Opportunities for intruders – part of the resources of intruders available to implement attacks on defender assets.

The share of investment – part of the opportunities aimed at protecting the assets of the company.

Percentage of attacks – the number of attacks that cybercriminals distribute between the security vectors of defenders according to previous successful attacks.

Successful attacks – attacks that can violate asset protection through security vectors.

Profit of defenders – monetary gain from improving the level of asset security, which in turn in creases the reputation, thereby improving the financial performance of the company.

Welfare of the attackers – a monetary advantage from the violation of the assets of the defenders.

The formed concepts should be included in the mathematical model, since they reflect the nature of the interaction of the parties to the conflict and influence the distribution of limited investment funds.

To get an idea of the dynamics of the attacker-defender interactions, a quantitative and integrative dynamic model with a suitable border, time horizon and a realistic interpretation of strategic decisions by individuals is needed.

The model consists of three submodels: Defender Submodel, Battlefield Submodel and Attacker submodel. The model was built on the following assumptions and limitations.

Assumption 1. The impact of cyberattacks on a firm's reputation.

There are both direct and indirect costs associated with cyber security breaches. Direct costs for companies include, for example, money spent on intrusion detection systems, overtime for hack recovery personnel, and, for example, lost productivity during virus attacks. However, these are the costs that companies face in the daily work of their business in the world of the Internet. The direct costs of cybersecurity are not included in the analyzed model.

The real financial damage from cyber security breaches is associated with indirect costs [73]. These can be losses caused by falling sales, weakening customer relationships and legal obligations. Indirect costs are difficult to measure, but they must be presented in the model, since they can significantly affect the company's income.

The company's reputation is fundamental. Loss of reputation is considered the indirect costs that the company incurs as a result of cyber-attacks. An ad or an article containing a security breach may affect their reputation and financial performance. An example of this is a virus attack on bank ATMs, which causes them to close for several hours, this may bother customers, but they probably will not change banks in connection with this incident. However, if the bank is hacked and customer data is distributed on the Internet, customers may well decide to start their own business elsewhere. In the latter case, the violation had a negative impact on the reputation and, consequently, on the market value of the company due to the real potential for loss of future revenue when customers change the service bank.

The analyzed model assumes the value for each of the three security vectors as the weight coefficient that they attach to their reputation, as well as the status of vector vulnerabilities and successful attacks. Modeling will provide an understanding of the value that the company attaches to cybersecurity to maintain its reputation.

Assumption 2. The capabilities of defenders and attackers are external parameters.

A firm's ability to invest in information security is limited by its finances. In particular, information security should compete with other projects for financing. Given budgetary constraints, the more difficult task for managing information security is not so much the general level of the required level of investment as the allocation of limited resources to protect against attacks [74].

Depending on the size of the company and the industry to which it belongs, the capabilities of firms will vary. The model assumes a relatively large company, since the budget for information security does not depend on the financial performance of the company. In other words, the budget for investing in information security in this case is fixed and affordable for each modeling period.

Opportunities for attackers are also assumed to be constant for each period. In a real system, hackers are criminal organizations that act in accordance with their own business model. Therefore, it is not known exactly how the attackers behave, and on what they build their business case and, therefore, how they form their resources for future attacks. The model reflects the behavior and capabilities of attackers described in the articles.

Assumption 3. The cost of a single attack. The cost of a single attack means the ratio of the capabilities of attackers and defenders. This parameter represents the damage that each attack does to the defenders. In other words, the cost of a single attack is how much money a defender needs to repel an attack.

In the model, the cost of a single attack is an exogenous variable. This option will increase the ability of attackers to determine the vulnerability status of each security vector.

Assumption 4. Type of attackers and type of attacks. Cyber-attacks can come from inside or outside the company. The model makes no distinction between internal and external attackers. Internal attackers include disgruntled and/or negligent employees who use a weak password to access the system or follow a link from a phishing site, not knowing that it is malicious software. Another type of attacker is an external one, generally including hacker organizations of criminals. In addition, the model does not break attacks into various types, for example, denial of service, phishing, viruses, ransomware, SQL injections, and so on.

Assumption 5. The cost of security for defenders. In the model, the cost of security that defenders bear when making an investment decision each period is reflected in the decision rule on the share of investments that they allocate for each security vector when it is violated.

The model does not reflect various financial indicators and does not use approaches to analyze each investment decision, such as: cost-benefit analysis, risk analysis, net present value (NPV), annual loss estimation (ALE), return on securities investment (ROSI) etc. The reason for this is that financial analysis would require a more complex model, including empirical data, to give greater accuracy to research.

The structure of the model represents both a qualitative display of the system, through causal relationships between variables, and its quantitative representation, by formally determining causal relationships through equations.

The system dynamics model contains three submodels:

– Defender Submodel;

– Battlefield Submodel;

– Attacker Submodel.

The Defender Submodel represents the structure of a firm's defense against malicious cyber-attacks that attempt to violate the security of its information asset. In each period, the defender makes a decision to determine his defense configuration. It is assumed that defenders have basic protection for each vector, and their security capabilities are designed to cover the additional security efforts resulting from security breaches.

We introduce the following notation for the variables and factors describing the Defender Submodel (**Table 2.5**).

Table 2.5 Formal designation used in Defender Submodels

Variable	Description
A_i^S	Successful Attacks
T^{RA}	Time to report Attack
NDA	Number of Dismissed Attacks
T^D	Dismissal time
D	Dismissed
R	Reports
FI_i	Fraction Investment Vector *i*
Rep	Reputation
BU	Building Up
T^{BUR}	Time to build up reputation
Adj	Adjustment
ER	Erosion
T^{RL}	Time reputation loss
R^B	Base reputation
V_i	Vector *i* Value
Vul_i	Vulnerability Vector *i*
DFP	Defenders Financial Performance
RMR	Reputation to money rate
BFP	Base financial performance
DAP	Defenders Accumulated Profit
IFP	Increasing Financial Performance

Defender protects his asset against three security vectors (*A*, *B* and *C*) that matter, which will be converted into reputation and then into financial results. In the model, security vectors are presented as the vulnerability state of each vector.

In case of successful attacks, a message is generated indicating the specific attack vector by which the target of the attack was achieved.

A description of the dynamics of successful attacks for each of the vector can be represented in the form of the following relationships:

$$\frac{d\left(A_i^{RS}\right)}{dt} = R_i - D_i, \quad R_i = A_i^S / T^{RA},$$

where R_i – increase in the number of successful attacks on a specific vector during the time required by the defender to report successful attacks (1 month); D_i – the number of reflected attacks reported, divided by the time required by the defenders to stop such attacks (1 month).

The share of the investment vector for each vector is calculated based on the reported successful attacks divided by the sum of the recorded successful attacks of all three vectors. The equation indicates that the defender will invest a share of investments in the *i*-th vector, which is equal to the total number of successful attacks received on this vector:

$$FI_i = A_i^{RS} \Big/ \sum_{i=1}^{3} A_i^{RS}.$$

Reputation is presented as a stock that accumulates during each modeling period. Reputation enhancement is the growth rate obtained by adjusting the reputation, which, in turn, is the result of the sum of the values of each security vector and their corresponding vulnerability result for each vector:

$$\frac{d(Rep)}{dt} = BU - ER,$$

$$BU = \begin{cases} Ad/T^{BUR}, \text{ if } Ad > 0; \\ 0, \text{ if } Ad \le 0, \end{cases} \quad ER = \begin{cases} \left|Ad/T^{RL}\right|, \text{ if } Ad < 0; \\ 0, \text{ if } Ad \ge 0. \end{cases}$$

Raising a reputation is the following decision-making rule: reputation growth rate will increase whenever the adjustment is positive. On the contrary, a negative adjustment (loss of reputation) means that the company is losing its reputation:

$$Ad = IR - Rep, \quad IR = R^B - \sum_{i=1}^{3} V_i \times Vul_i.$$

Financial Performance of Defenders. Financial indicators of defenders are determined by the current reputation and the ratio of the level of reputation to funds, which shows how much the reputation of the company is estimated in relation to its financial indicators:

$$DFP = (RMR \times Rep) + BFP.$$

Defenders Profit determined by financial indicators, which is necessary for the analysis of policy options:

$$\frac{d(DAP)}{dt} = IFP.$$

The Battlefield sub-model is a segment of the model in which defenders and attackers interact with their respective capabilities and investment decisions. The main components of this submodel are Vulnerability and Successful attacks of each security vector. In the description of the submodel of the battlefield, the following notation of variables is used (**Table 2.6**).

⬢ **Table 2.6** Description of Variable Submodels of the Battlefield

Variable	Description
C^A	Attackers Capabilities
AF_i	Fraction of Attack Vector *i*
C^{UA}	Attack Unitary Cost
C^D	Defenders Capabilities

Vulnerability of attack vectors indicates the level of security for each of the vectors. If the vulnerability is positive, it means that the system is weak in security. Vulnerability is determined by the following expression:

$$Vul_i = \left(C^A \times AF_i \times C^{UA}\right) - \left(C^D \times FI_i\right).$$

In essence, the vulnerability is determined by the difference between the resources that the attacker directs to the corresponding vector of attacks and the resources that the defender allocates to fix security flaws on the same vector.

The resources of an attacker are determined by his abilities, multiplied by the fraction of the capabilities allocated for attacking the vector, and by money, for the attack equivalent to each attack. Similarly, the resources of the defender are the result of the multiplication of his abilities and the share intended to protect the vector after hacking.

Successful attacks are important for this model, as they will trigger future investment decisions for both opponents. Successful attacks are calculated as follows:

$$SA_i = \begin{cases} \left(C^A \times AF_i\right) - \left(\left(C^D \times AF_i\right) / C^{UA}\right), \text{ if } Vul_i > 0; \\ 0, \text{ if } Vul_i \le 0. \end{cases}$$

This formulation entails that if the vulnerability of the vector is below zero, there will be no successful attacks, since the defender has equal or superior capabilities than the attacker, and he is able to stop all attacks. On the other hand, if the vulnerability of a vector is above zero, there will be successful attacks.

Multiplying the defender's capabilities by the share of invested funds, and then divided by the cost of a single attack, indicates the number of attacks that the defender can reflect in case of a security violation. Thus, the difference between the number of attacks carried out for each vector and the number of attacks that the defender can repel is equal to the total number of successful attacks.

The attacker is aimed at the company and makes some efforts to implement attacks. Since the attacker does not know where to aim in order to gain profit, he uses the initial distribution of successful attacks to determine the distribution of vulnerabilities by vectors.

The attacker identifies and uses the weakest link, i.e. the security vector with the lowest protection. If the attacker succeeds, he will make a profit, which will mean lower financial performance for the defender. The attacker does not act indiscriminately; rather, he attacks only when it is beneficial to him.

Successful historical attacks in the attacker's model prompt to attack the weakest link and not neglect other vectors, allocating a smaller part of the resources for their attack. It is assumed that the attacker obtains the same utility for using all security vectors.

To represent the relations that determine the attacker's behavior, the following notation of variables has been introduced (**Table 2.7**).

Table 2.7 Variable designations for an attacker submodel

Variable	**Description**
A_i^{AS}	Accumulated Successful Attacks Vector *i*
B	Breaches
A_i^S	Successful Attacks Vector *i*
T^{RA}	Time to report attack
V_i^P	Past value *i*
S_i	Switch *i*
P^A	Attackers Performance
B_i	Breaches Vector *i*
W^{AA}	Accumulated Attackers Wealth
W^{IA}	Increasing Attackers Wealth

Accumulated successful attacks. The sum of the accumulated successful attacks of each vector allows the attacker to determine the weakest link and determine the solutions for the next attack in order to use the most vulnerable security vector. The designation *i* indicates the vectors *A*, *B* and *C*.

$$\frac{d\left(A_i^{AS}\right)}{dt} = B_i, \quad B_i = A_i^S / T^{RA}.$$

The increase in this indicator is determined by successful attacks in the vector, divided by the time it takes for attackers to report attacks (1 month).

Share of attack vectors – are decisions made by attackers as a result of accumulated successful attacks on each vector. For the weakest link strategy to work in this model, attackers must switch from one vector to another when the current vector is not good enough for him to continue to attack him.

For this reason, the parameter of the past value is used to save the previous value of the previous period in order to be able to compare the current value of the attack with the past value of the accumulated successful attacks for the last period and determine whether it increases or decreases in order to decide whether or not to change the vectors.

$$V_i^P(t) = A_i^{AS}(t-1).$$

Switch parameter is a condition that indicates that when the comparison of the current value with the previous value is less than 1, then the switch becomes zero, and it is not advantageous for the attacker to continue using this vector and move on to another. The conditional value is 1, not zero, since 1 is a threshold for evaluating the differences between the two values, which must be at least equal to one to justify the change.

This is an example of calculating the attack fraction of the vector *A*, but for the other vectors the same:

$$S_i = \begin{cases} 0, \text{ if } A_i^{AS} - V_i^P < 1; \\ 1, \text{ if } A_i^{AS} - V_i^P \geq 1, \end{cases}$$

$$A_i^F = S_i \times A_i^{AS} \Big/ \sum_{i=1}^{3} \left(S_i \times A_i^{AS}\right).$$

Whenever an attacker decides to stop attacking one vector and switch to another, investments in the other two vectors will increase.

Attacker performance – this is the sum of violations of all vectors multiplied by the cost of a single attack:

$$P^A = \sum_{i=1}^{B} B_i \times C^{UA}.$$

The «welfare» of attackers is determined by financial indicators; this stock was created for analysis purposes in the following scenario and policy options analysis. The influx of wealth of attackers is a function of the productivity of attackers.

$$\frac{d(AAW)}{dt} = IAW.$$

The choice of a particular methodology should be based on a comparison of the most common modeling methodologies.

Thus, it is proposed to conduct a comparison according to the following criteria:

– the time and effort required to apply the methodology of modeling and designing the current model with the participation of future users;

– user requirements. The amount of technical knowledge and the level of training necessary for the user to understand and use the model;

– studying time. Time and effort for a typical user to study the designed model and the rules for its use;

– model flexibility. The simplicity with which a developer can change the model to include a new variable or change the variables used;

– number of existing analog models with functions that can be adapted to be used as part of the behavior model of security agents;

– transparency. The simplicity with which the user can discover in the model everything that can affect the simulation results.

The results of the comparison of various methodologies are presented in **Table 2.8**. It should be noted that the first three criteria should be low, and the last three criteria should be high.

Table 2.8 Compliance of modeling methodologies with comparison criteria

	Time to create a model	**User requirements**	**Study time**	**Flexibility**	**Availability of model library**	**Transparency**
Game theory	L	L-H	L-H	M	H	L-H
Agent Modeling	M-H	L-M	L-M	M-H	L-M	M-H
Dynamic systems	M	H	H	M	M	M
System dynamics	L	L	L	H	L	H
Data Driven Models	M	M	L	M	M	H

Note: *L – low, M – medium, H – high*

Based on a set of comparison criteria for agent behavior modeling methodologies, system dynamics may turn out to be an alternative to game-theoretic modeling of agent behavior. The advantages of system-dynamic modeling also speak in favor of this choice. The methodology of system-dynamic modeling allows:

– to detect the emergent properties of the investigated system behavior. System-dynamic models provide a way to study the formed behavior of agents based on the relatively simple rules of behavior of an individual agent. This approach allows to obtain and further study the synergistic properties of antagonistic agents in the process of cyber conflict;

– to determine the most important parameters in the system dynamics: it is necessary to determine the set of input data in order to understand their influence on the output data. The system-dynamic model allows you to evaluate the impact of each input parameter on the result of the system's functioning and rank them depending on the degree of influence, and subsequent analysis of the model's sensitivity will support the decision to include one or another factor in the model;

– to prepare quantitative assessments of qualitative ideas: systemic dynamic models allow the user to convert a qualitative understanding of agent interactions into quantitative assessments of the effectiveness of the implementation of a particular scenario of behavior in the process of cyber conflict;

– to predict the long-term consequences of decisions for a certain circuit of business processes;

– to support the use of the model and provide system administrators with a set of tools for organizing training for personnel in decision-making in difficult conditions of cyber conflict. In particular, system dynamics is a method for improving learning in complex security systems, especially large infrastructure projects. The study of complex dynamic systems requires not only technical means to create mathematical models, since these tools are applied both to human behavior and to physical and technical systems.

The results obtained from the analysis of the comparison table are explained primarily by the selection of appropriate comparison criteria. These criteria reflect the basic requirements on the part of developers of security agent behavior models. It should be borne in mind that for other subject areas and other tasks, the set of comparison criteria can be changed, which will lead to different selection results.

The second factor influencing the results of the comparison is the subjective nature of the assessments of the conformity of a particular methodology to the established criteria. In addition, these estimates are purely qualitative in nature, and the boundaries between the low, medium, and high values of compliance with the criterion are not fixed.

The subjective choice of criteria and their values determine not only the features of the proposed approach, but also its limitations. As ways to address these shortcomings of the approach to justifying and choosing a modeling methodology, the following can be proposed.

First of all, the use of expert assessment methods that provides quantitative assessments of the rationale for the choice, namely, the determination of the required number of experts and the degree of consistency of their assessments, which allows to talk about the stability of the group assessment of the chosen methodology. As the second way, allowing passing to a quantitative assessment of the justification of a choice, one can use the theory of fuzzy sets that transform the qualitative values of the criteria into quantitative estimates for their subsequent processing. It should be noted that the use of fuzzy sets in the field of cybersecurity is mainly associated with the assessment of risks of threats.

2.5 METHODOLOGICAL FOUNDATIONS FOR THE DEVELOPMENT OF A CYBER THREAT CLASSIFIER

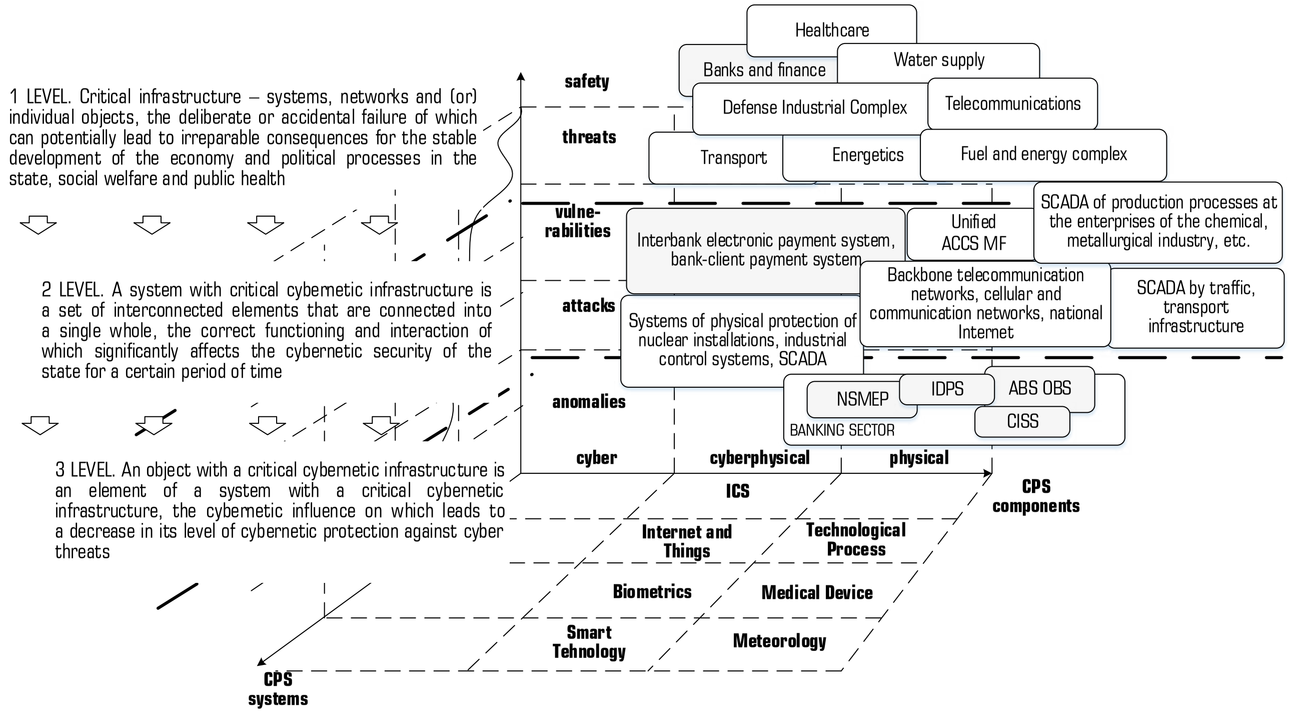
The development of computing resources and «G» technologies has predetermined the rapid growth of the Internet of things based on the synthesis of physical systems and Internet technologies. Given the fact that there is no single universally accepted definition of cyberphysical systems, a rather general definition of a cyberphysical system as a system used to monitor and control objects of a physical nature (the physical world) is given in [75]. These systems are perceived as a new generation of embedded control systems. In addition, systems in which networks of sensors and actuators are integrated are also considered cyberphysical systems [76]. Due to the dependence on IT systems, cyber-physical systems can be defined as IT systems that are integrated into applications of the physical world [77]. This integration is the result of advances in information and communication technology (ICT) to improve interaction with physical processes.

All these definitions emphasize the constant and intense interaction between the cyber and physical worlds. However, their development also determined a new direction in the development and/or modification of old threats, which is not only manifested in the possibility of hacking and unauthorized access to confidential (personal) information of users, but also in the possibility of conducting an «energy apocalypse». This approach allows cybercriminals to use cyberphysical systems to obtain a synergistic effect from the implementation of threats in cyberspace as a whole. There are many tasks that dictate the need for a unified approach based on the construction of classification of threats. These tasks include analyzing deviations from the normal operation of the security circuit in cyberphysical systems, ensuring the stable operation of the security circuit in cyberphysical processes, and preventing hacking of the security system. The construction of a classifier of threats should be carried out taking into account their synergy and hybridity for all security components, namely, information security (IS), cybersecurity (CS) and security of information (SI). The classifier should reflect the need to integrate security components with social engineering methods and take into account the lack of funds to ensure the required level of security.

Publications dealing with the development of methodological foundations for constructing classifiers of threats to cyberphysical systems can be divided into three groups. The first group combines publications describing various cyberphysical systems and their features and characteristics that make them vulnerable to various kinds of threats. The second group includes publications on a variety of threats and attacks directed specifically at cyber-physical systems. The publications of the third group describe various approaches to the construction of taxonomy and classification, which, ultimately, lead to the construction of threat classifiers for cyberphysical systems.

The most significant article of the first group is [75], in which existing studies on the safety of cyberphysical systems (CPS) are collected and systematized within a single structure. The proposed structure is a three-dimensional system of orthogonal coordinates. The first axis corresponds to the well-known classifications (taxonomies) of threats, vulnerabilities, attacks and security controls. The second axis corresponds to the components and subsystems in terms of their nature, namely, cybernetic (computer information), physical and cyberphysical. The latter exhibits synergistic properties that were not possessed by the elements or subsystems of the first two. And finally, the third axis corresponds to the reflection of the integral (synergetic) functions of cyberphysical systems, as well as their manifestation in various typical cyberphysical systems (for example, intelligent networks, medical CPS and intelligent machines, and mechanisms). In **Fig. 2.5**, the relationship of the proposed structure with critical cybernetic information systems (CCIS) is proposed, using the banking sector as an example.

It is noted that the designed CPS model can be either abstract to show the general interactions of the CPS application, or specific to capture any details when necessary. This representation allows you to build a model that is abstract enough to be applicable to various heterogeneous CPS applications and to obtain a modular representation of closely related and interacting CPS components. In this case, the formation and manifestation of synergistic properties in the process of functioning are provided. This abstract separation allows you to build a systematic understanding of CPS security and highlight potential attack sources and defenses. The paper argues that identifying differences between traditional IT systems and cyberphysical systems is key in understanding CPS security issues and the subsequent construction of threat classifiers for such systems.



1 LEVEL. Critical infrastructure – systems, networks and (or) individual objects, the deliberate or accidental failure of which can potentially lead to irreparable consequences for the stable development of the economy and political processes in the state, social welfare and public health

2 LEVEL. A system with critical cybernetic infrastructure is a set of interconnected elements that are connected into a single whole, the correct functioning and interaction of which significantly affects the cybernetic security of the state for a certain period of time

3 LEVEL. An object with a critical cybernetic infrastructure is an element of a system with a critical cybernetic infrastructure, the cybernetic influence on which leads to a decrease in its level of cybernetic protection against cyber threats

safety
threats
vulne-
rabilities
attacks
anomalies
cyber
cyberphysical
physical
CPS
components
CPS
systems
Healthcare
Banks and finance
Water supply
Defense Industrial Complex
Telecommunications
Transport
Energetics
Fuel and energy complex
Interbank electronic payment system, bank-client payment system
Unified
ACCS MF
SCADA of production processes at the enterprises of the chemical, metallurgical industry, etc.
Backbone telecommunication networks, cellular and communication networks, national Internet
SCADA by traffic, transport infrastructure
Systems of physical protection of nuclear installations, industrial control systems, SCADA
NSMEP
IDPS
ABS OBS
CISS
BANKING SECTOR
ICS
Internet and Things
Technological Process
Biometrics
Medical Device
Smart Tehnology
Meteorology

Fig. 2.5 Relationship of CCIS with CPS

Four specific cyberphysical systems are specifically considered, namely, power supply networks, medical systems, smart cars and industrial facilities control systems. For these systems, the issues of communication in these systems and their safety are discussed in detail. It is emphasized that security control is usually associated with mechanisms such as cryptography, access control, intrusion detection and many other solutions commonly used in IT systems. These mechanisms are very important for protecting the infrastructure of information and communication technologies. It is noted that security solutions require solutions that take into account cyber-physical aspects, and they can be supplemented by IT security solutions.

Ensuring the security of CPS is associated with various problems, one of which is an understanding of potential threats [76]. Knowing who/from what CPS protection is organized is equally important for understanding existing vulnerabilities and attack mechanisms. A security threat is defined as «a set of circumstances that could lead to loss or harm» [77].

In [75], five factors are identified for each threat: source, target, motive, attack vector and potential consequences. The source of the threat is the initiator of the attack.

Sources of threats are divided into three types [78–83]:

– warring threats (intentions of individuals, group organizations or states/nations);

– random threats (threats that were caused by accident or using CPS components);

– environmental threats, including natural disasters (floods, earthquakes), man-made disasters (fires, explosions) and interruptions in the supporting infrastructure (power outages or loss of communication).

Goals are CPS applications, their components, or users. CPS attackers usually have one or more reasons to launch an attack: criminal, spyware, terrorist, political, or cyber warfare [84]. A threat can perform one or more of the four mechanisms of a successful attack: interception, interruption, modification, or fabrication [79]. The consequences of an attack may be a violation of the confidentiality, integrity, availability, confidentiality or security of the CPS.

Potential threats and vulnerabilities are investigated for the selected four applications of cyberphysical systems. The work contains summary tables reflecting the influence of each of the five factors noted on a particular type of cyberphysical system, as well as a list of characteristic attacks undertaken against such systems. Despite the fact that the listed factors can be considered as the foundation for constructing a classifier of threats to cyberphysical systems, the issues of taking into account the synergistic effects of the functioning of such systems have not been considered.

In general, the contribution of the mentioned work to the problem of constructing CPS threat classifiers can be formulated as follows:

– the CPS security system, designed to distinguish between cyber, cyberphysical and physical components in this system is proposed;

– the potential sources of threats and their motives are investigated;

– existing vulnerabilities are presented and significant reasons for their occurrence are highlighted using real examples;

– a review of recorded attacks on CPS was conducted to identify the main vulnerabilities and components susceptible to threats;

– a comparative analysis of existing control mechanisms has been carried out and unresolved problems and problems in various CPS applications have been identified.

In [78], three key issues for protecting cyber physical systems are discussed: understanding the threats and possible consequences of attacks, identifying the unique properties of cyber physical systems and their differences from traditional IT security, and discussing security mechanisms applicable to cyber physical systems. In particular, security mechanisms are analyzed for: prevention, detection and recovery, resilience and deterrence of attacks.

A distinctive feature of the work is the development of an adversary model as a way to understand the extent of the problem and assess the risks. The work contains descriptions of some potential attackers, their motives and resources. An analysis of the behavioral aspects of attackers was made in [85, 86].

The work notes that the goal of cybercriminals is to compromise computers wherever they can be found (even in control systems). Attacks by cybercriminals may not necessarily be targeted. Cybercriminals may not have the intent to harm control systems, but their actions can cause negative side effects. For example, control systems infected with malware may not work properly.

Insiders are currently the main source of targeted computer attacks on control systems [87]. These attacks are important from a security point of view, because they are caused by persons with authorized access to computers and networks used by management systems. Therefore, even if control networks are completely isolated from public networks (and the Internet), insider attacks will still be possible. Since disgruntled employees tend to act alone, the potential consequences of their attacks may not be as devastating as the potential damage done by larger organized groups.

Terrorists, activists and organized crime groups are another potential threat to control systems. Attacks on extortion control systems are not new. Cyber-attacks are a natural development of physical attacks: they are cheaper, less dangerous for an attacker, not limited by distance, they are easier to copy and coordinate.

States can also be a potential threat to governance systems. In general, it is not surprising that most military powers learn the technology of future attacks, including cyber-attacks against the physical infrastructure of other countries.

The work emphasizes that the main objective of the research is to identify and classify a new type of attacks that are possible in control systems, and to study their possible consequences. For example, attackers can launch unique attacks on control systems (that is, attacks that are not possible in traditional IT systems). One possible example would be resonant attacks. In a resonant attack, an attacker who compromises some sensors or controllers will cause the physical system to oscillate at its resonant frequency. In [88], based on the definition of a cyberphysical system as a distributed control system with strict time constraints consisting of physical and cyber components, the differences between the IT system and the cyberphysical system are formulated. Physical Interface: Having a physical interface is what makes CPS security especially difficult. Unlike a standalone IT system, a security breach in a CPS system has disastrous consequences. An attacker can use a physical interface to undermine the security of CPS without the need to violate the access control mechanism. In traditional IT security, this can only happen if data is transmitted over an open network.

Control system: CPS is based on one or more core control networks, which are often integrated with a physical sensor/actuator, which differs markedly from the traditional point of view of IT security. Supervisory control and data acquisition systems (SCADA) are an integral part of modern industrial infrastructure. Unsurprisingly, vulnerabilities in this management network remain an attractive place for cyber-attacks that continue to grow due to SCADA systems connected to the Internet [89]. A feature of the analyzed work is not only the classification of attacks, but also its connection with security standards. In addition, modern hybrid attacks on state-level computer systems do not just damage an isolated machine or disrupt the operation of a single corporate system [90]. Instead, new attacks target infrastructure, which is an integral part of the economy, national defense, and everyday life [91]. Studies of cyberphysical systems have shifted the focus from developing the optimization task of these computing components to the interaction involved between physical media and the computing elements with which they interact [92]. A classification consisting of four dimensions was proposed in [93], which allows one to simultaneously consider issues of both the functioning of the network and issues related to computer attacks. The first dimension of the classification covers the attack vector and the main scenario of the attack. The second dimension of classification identifies an attack by its primary purpose. Vulnerabilities are classified in the third dimension of the classification, and payloads in the fourth taxonomy. Similarly, the authors present an information security risk analysis methodology that links the assets, vulnerabilities, threats and controls of an organization. The approach uses a sequence of matrices that reflect the correlation of various elements in a risk analysis. The data are aggregated and cascaded by matrices in order to correlate assets with controls in such a way as to obtain priority ranking of controls based on the assets of the organization [94].

In addition, cyber-physical incidents were discussed and classified in [95] based on sectors, sources and impacts of incidents. This document provides an example of how organizing the process of collecting information about cyber incidents can be used by victims of cyber-attacks. In addition, an attempt is described to help understand the threat of cyber incidents for various purposes, which may be useful to increase organizational focus from the point of view of cyber incident. In addition, the security ontology for investigating incident analysis [96] allows one to organize a classification similar to that presented in [97].

In the proposed classification, the stages of incidents were investigated taking into account additional extensions that reflect various categories of the entity involved in attacks and attack relationships. So, the authors distinguished the following classes of entities: an attacker, a vulnerability, a tool, a target, an action, goals, and an unauthorized result. Attackers use tools to perform actions that exploit target vulnerabilities. In [98], models of virtual control system environments (VCSE) are presented, which illustrates the corresponding parts of CPS and their threats. They are designed to analyze the influence of physical factors. Models were built from real, simulated and emulated components that were vulnerable to actual, simulated malicious and other hostile activities. In addition to the dynamic basis of cyber terrorism, a structure was proposed in [99] that describes the main components of cyber terrorism. Cyber terrorism was defined by a structure reflecting six points of view: motivation, goal, attack method, subject area, criminal actions and attack effects.

The classification of cyber-attack and defense mechanisms for emergency management networks aims to support a common understanding of the associated cyber-attack and defense mechanisms. Attack mechanisms are classified according to three aspects, according to the network, according to the attacked functions and attack factors, while the defense mechanism is determined by the type of protection, the degree of distribution and organizational elements [100]. In addition, the problems of cybersecurity in emergency management are divided into three groups determined by the criticality of time (refers to emergency situations), when decisions must be made and quickly transmitted. The National Institute of Standards and Technology (NIST) [101] presented a framework focused on using business drivers to guide cybersecurity activities and address cybersecurity risks as part of the organization's risk management processes. The classification structure is represented by three parts: the core of the structure, the profile of the structure, and the levels of implementation of the structure. The core of the structure is a set of cybersecurity measures, outcomes and information guides that are common to critical infrastructure sectors, providing detailed guidance for developing organizational personality profiles. Using the profile, the structure is designed to help the organization bring its cybersecurity activities in line with business requirements, acceptable risks and resources. Tiers provide a methodology for organizations to understand and consider the characteristics of a cybersecurity risk management approach. In addition, a threat-based mathematical quantitative structure is used in [102], which is used to evaluate and design the security of CPSTo counter each element of the threat, it is proposed to be guided by the following three principles:

– principle 1: focusing on a critical system should include only basic functions;

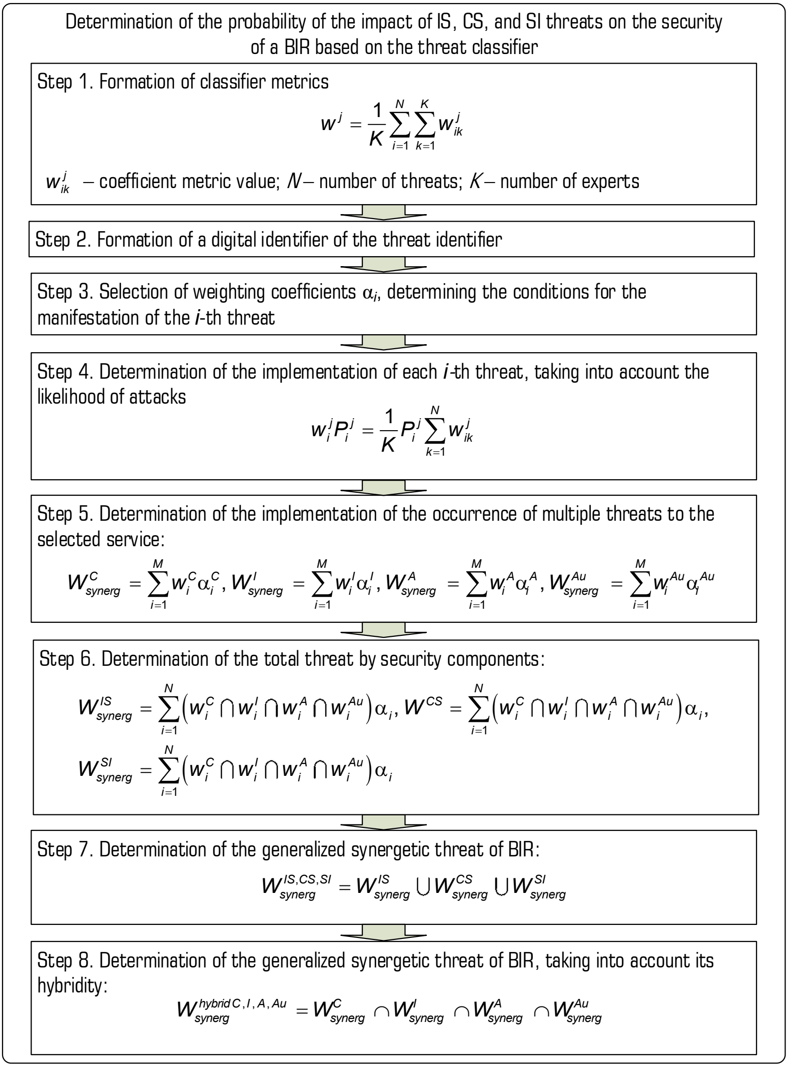
– principle 2: the movement of key elements of the assets necessary for the mission, and security control, which is difficult for an attacker to achieve physically and logically (to reduce accessibility);

– principle 3: responding, detecting, adapting and misleading attackers by introducing system elements with dynamic response technologies (to counter the attackers' capabilities).

The fundamental work in Ukraine, devoted to the construction of classification systems and classifiers of threats in the field of cybersecurity, is undoubtedly the work [103]. The paper presents the results of the analysis of modern protection of state information resources (SIR) in information and telecommunication systems. At the same time, the emphasis in the work is placed on the regulatory support for the SIR, the legal aspects of the formation of the SIR are described in detail, and new terms and definitions of the problems of their protection are introduced. A significant drawback is the lack of communication of threats with the OSI model, which allows you to identify critical penetration points.

In [104], the authors propose an improved version of the classifier of threats to banking information as one of the resources of critical cybernetic information systems (CCIS) of the state, taking into account their synergies and synergies of security components. **Fig. 2.6** shows a block diagram of the proposed solution.

Thus, the analysis showed that the approaches considered do not take into account the combination of modern threats that are hybrid and synergistic with the elements of the cyberspace infrastructure of companies/organizations. Existing approaches practically do not take into account the economic aspects of ensuring security, which limits the minimization of economic costs for the construction of a comprehensive information protection system. It is the neglect of the economic aspects of security in the construction of the classifier of threats that makes the proposed study relevant.



Determination of the probability of the impact of IS, CS, and SI threats on the security of a BIR based on the threat classifier

Step 1. Formation of classifier metrics

$$w^j = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ik}^j$$

w_{ik}^j – coefficient metric value; N – number of threats; K – number of experts

Step 2. Formation of a digital identifier of the threat identifier

Step 3. Selection of weighting coefficients α_i, determining the conditions for the manifestation of the i-th threat

Step 4. Determination of the implementation of each i-th threat, taking into account the likelihood of attacks

$$w_i^j P_i^j = \frac{1}{K} P_i^j \sum_{k=1}^{N} w_{ik}^j$$

Step 5. Determination of the implementation of the occurrence of multiple threats to the selected service:

$$W_{synerg}^{C} = \sum_{i=1}^{M} w_i^C \alpha_i^C,\ W_{synerg}^{I} = \sum_{i=1}^{M} w_i^I \alpha_i^I,\ W_{synerg}^{A} = \sum_{i=1}^{M} w_i^A \alpha_i^A,\ W_{synerg}^{Au} = \sum_{i=1}^{M} w_i^{Au} \alpha_i^{Au}$$

Step 6. Determination of the total threat by security components:

$$W_{synerg}^{IS} = \sum_{i=1}^{N}\left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}\right)\alpha_i,\ W^{CS} = \sum_{i=1}^{N}\left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}\right)\alpha_i,$$

$$W_{synerg}^{SI} = \sum_{i=1}^{N}\left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}\right)\alpha_i$$

Step 7. Determination of the generalized synergetic threat of BIR:

$$W_{synerg}^{IS,CS,SI} = W_{synerg}^{IS} \cup W_{synerg}^{CS} \cup W_{synerg}^{SI}$$

Step 8. Determination of the generalized synergetic threat of BIR, taking into account its hybridity:

$$W_{synerg}^{hybrid\,C,I,A,Au} = W_{synerg}^{C} \cap W_{synerg}^{I} \cap W_{synerg}^{A} \cap W_{synerg}^{Au}$$

Fig. 2.6 Determining the probability of threats based on a synergistic model of threats

To create a threat model, they usually use the adapted CIA triad model (confidentiality, integrity, availability), which is the basis for its further modifications in practical models (Hexad Parker model, 5A model, STRIDE model, etc.). However, in the conditions of post-quantum cryptography (in the context of the emergence of a fullscale quantum computer), US NIST experts question the provision of the required level of security with modern symmetric and asymmetric cryptosystems [105].

In addition, the rapid growth and use of «G» technologies can significantly change the vector of the use of cyberspace as the main channel for transmitting information between cyber systems and information and communication systems.

Such changes significantly reduce the level of security and can practically reduce it to zero. Under such conditions, it is necessary to consider the complex of threats – their combination and hybridity, leading to the appearance of a synergistic effect with a subsequent increase in the likelihood of a threat based on a synthesis with social engineering methods.

In [106], the authors proposed a fundamentally new approach to the methodology for constructing security systems based on the synergetic threat model, which provides the formation of methodological foundations for constructing a classifier of modern threats to cyberphysical systems.

In **Fig. 2.7**, a block diagram of the synergetic model of synthesis threats to information-critical cybernetic systems (on the example of banking sector organizations) and CFS is proposed.

In accordance with ISO/IEC 27001:2013, threats are classified as intentional, incidental and/or environmental. Typical examples include technical failures, unauthorized actions, software interference, physical damage, compromised functions, etc.

However, the standard, like other normative international acts, does not consider the synergy and hybridity of modern threats, their combination with social engineering methods, which significantly increases the risk of the threat. The proposed approach takes into account the possibilities of modern threats, their synergy and hybridity, the possibility of integration with social engineering methods. To design a classifier of threats to cyberphysical systems, **Fig. 2.8** provides a block diagram of the methodological foundations of a unified classifier taking into account the synergetic model of threats and economic costs of ensuring the required level of security.

Let us consider in more detail the proposed approach to the formation of a classifier of threats. At the first stage, experts are invited, using their experience, to form tuples of a threat classifier based on 5 platforms.

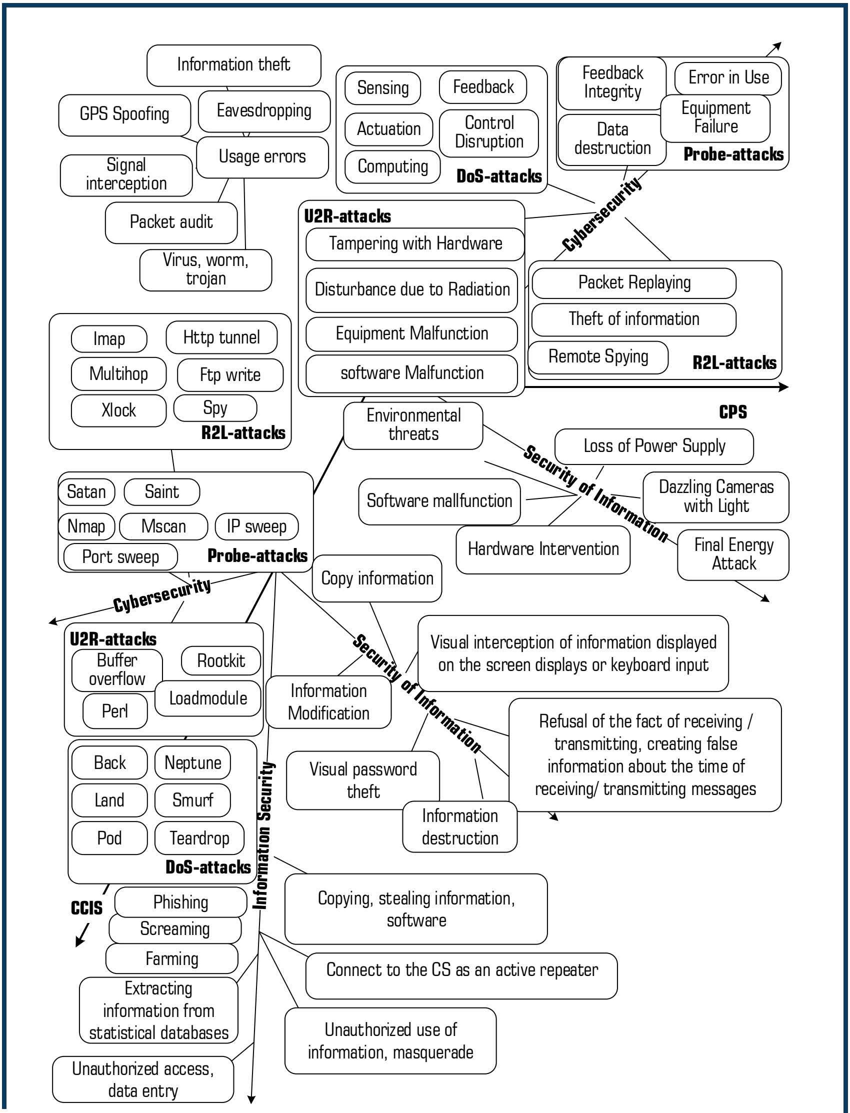
The first platform determines the criticality level of the threat (critical, high, medium, low, very low), which allows you to calculate the economic «profitability» of critical threats in step 5.

The second platform defines the attitude towards the security component (information security (IS), cybersecurity (CS), security of information (SI)), which allows you to get an assessment of the synergistic effect on one of the threat components in step 5.

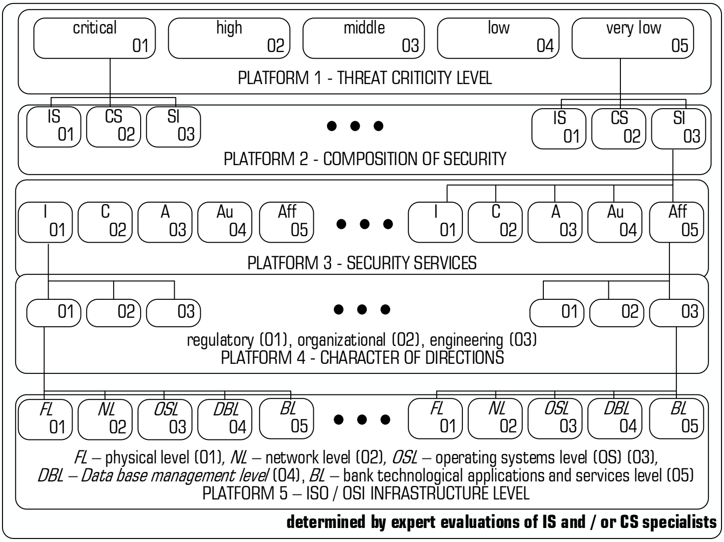
The third platform determines the direction of the threat to security services (integrity, confidentiality, accessibility, authenticity and involvement), which allows you to get an assessment of the impact of several threats on security services in step 4 and determine the direction vector of the impact on infrastructure elements.

The fourth platform determines the nature of the directions of the impact of threats (regulatory, organizational, engineering).

The fifth platform provides an assessment of focus on infrastructure elements and allows you to «identify» critical points in an integrated information security system (IISS). Moreover, for the objectivity of expert judgments, we use the weighting coefficients of expert competence (k_k), presented in **Table 2.9**.



⬡ **Fig. 2.7** Block diagram of a synergistic model of synthesis threats on CCIS and CFS


critical 01
high 02
middle 03
low 04
very low 05
PLATFORM 1 - THREAT CRITICITY LEVEL
IS 01
CS 02
SI 03
• • •
IS 01
CS 02
SI 03
PLATFORM 2 - COMPOSITION OF SECURITY
I 01
C 02
A 03
Au 04
Aff 05
• • •
I 01
C 02
A 03
Au 04
Aff 05
PLATFORM 3 - SECURITY SERVICES
01
02
03
• • •
01
02
03
regulatory (01), organizational (02), engineering (03)
PLATFORM 4 - CHARACTER OF DIRECTIONS
FL 01
NL 02
OSL 03
DBL 04
BL 05
• • •
FL 01
NL 02
OSL 03
DBL 04
BL 05
FL – physical level (01), NL – network level (02), OSL – operating systems level (OS) (03),
DBL – Data base management level (04), BL – bank technological applications and services level (05)
PLATFORM 5 – ISO / OSI INFRASTRUCTURE LEVEL
determined by expert evaluations of IS and / or CS specialists

STEP 1. FORMING METRIC THREAT COEFFICIENTS FOR ICS AND CPS

$$w_{ICS}^{j}=\frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K}w_{ICSik}^{j},\ w_{CPS}^{j}=\frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K}w_{CPSik}^{j}$$

STEP 2. FORMATION OF WEIGHT COEFFICIENTS OF CONDITIONS OF MANIFESTATION OF THREATS FOR ICS AND CPS

$$\alpha_{i}^{ICS},\ i\in[0{,}067;0{,}133;0{,}2;0{,}267;0{,}333],\ \alpha_{i}^{CPS},\ i\in[0{,}067;0{,}133;0{,}2;0{,}267;0{,}333]$$

STEP 3. DETERMINING THE IMPLEMENTATION OF EVERY THREAT FOR ICS AND CPS

$$w_{ICSi}^{j}P_{ICSi}^{j}=\frac{1}{K}P_{ICSi}^{j}\sum_{k=1}^{N}w_{ICSik}^{j},\ P_{ICSi}^{j}\in\left\{\alpha_{i}^{ICS}\right\},\ w_{CPSi}^{j}P_{CPSi}^{j}=\frac{1}{K}P_{CPSi}^{j}\sum_{k=1}^{N}w_{CPSik}^{j},\ P_{CPSi}^{j}\in\left\{\alpha_{i}^{CPS}\right\}$$

STEP 4. DEFINITION OF IMPLEMENTATION OF SEVERAL THREATS TO THE SECURITY SERVICE

$$W_{ICS\ synerg}^{C}=\sum_{i=1}^{M}w_{ICSi}^{C}\alpha_{i}^{ICSC}\bigcup W_{CPS\ synerg}^{C}=\sum_{i=1}^{M}w_{CPSi}^{C}\alpha_{i}^{CPSC}\ldots$$

$$W_{ICS\ synerg}^{Aff}=\sum_{i=1}^{M}w_{ICSi}^{Aff}\alpha_{i}^{ICSAff}\bigcup W_{CPS\ synerg}^{Aff}=\sum_{i=1}^{M}w_{CPSi}^{Aff}\alpha_{i}^{CPSAff}$$

STEP 5. DEFINITION OF THE TOTAL THREAT TO COMPOSITE SECURITY

$$W_{synerg}^{IS}=\sum_{i=1}^{N}\left(w_{ICSi}^{C}\bigcap w_{ICSi}^{I}\bigcap w_{ICSi}^{A}\bigcap w_{ICSi}^{Au}\bigcap w_{ICSi}^{Aff}\right)\alpha_{i}^{ICS}\bigcup$$

$$\bigcup\sum_{i=1}^{N}\left(w_{CPSi}^{C}\bigcap w_{CPSi}^{I}\bigcap w_{CPSi}^{A}\bigcap w_{CPSi}^{Au}\bigcap w_{CPSi}^{Aff}\right)\alpha_{i}^{CPS}$$

STEP 6. DEFINITION OF ECONOMIC COSTS FOR ATTACK PREVENTION

$$Tr_{ICSR}^{A}=\left\{Tr_{i}\left|\left(P_{i}^{A}-C_{i}^{A}\right)>0\right.\right\}\ \forall Tr_{i}\in Tr\Rightarrow Tr_{L}^{ICS}=\arg\max_{\forall Tr_{l}\in Tr_{C}^{D}}K_{l}^{D}\times K_{l}^{A}$$

$$Tr_{CPSR}^{A}=\left\{Tr_{i}\left|\left(P_{i}^{A}-C_{i}^{A}\right)>0\right.\right\}\ \forall Tr_{i}\in Tr\Rightarrow Tr_{L}^{CPS}=\arg\max_{\forall Tr_{l}\in Tr_{C}^{D}}K_{l}^{D}\times K_{l}^{A}$$

automatically determined based on mathematical expressions

Fig. 2.8 Block diagram of the threat classifier

⬢ **Table 2.9** Expert competency weight

No.	Expert Qualifications	Weight value (k_k)
1	International expert in the field of IS, CS, SI	1.0
2	National expert in the field of IS, CS, SI	0.95
3	Certified international specialist in the field of IS, CS, SI	0.9
4	Full doctor of science in the field of IS, CS, SI	0.9
5	Director of security service	0.85
6	Doctor of Philosophy in the field of IS, CS, SI	0.8
7	Security officer	0.7
8	System administrator	0.6
9	Security engineer	0.5
10	Graduate student in the field of IS, CS, SI	0.4

The total score of the *z*-th threat is determined by the number of experts according to the expression:

$$\widetilde{x_i} = \frac{\sum_{k=1}^{K} x_k \times k_k}{K}, \tag{2.3}$$

where x_k is the assessment of the of the *i*-th threat by the *k*-th expert; k_k – expert competency level; K is the number of experts.

A measure of the consistency of expert assessments is the variance, which is determined by the expression:

$$\sigma_x^2 = \frac{1}{K}\sum_{k=1}^{K} k_k\left(x_k - \widetilde{x_i}\right)^2. \tag{2.4}$$

The statistical probability of the obtained results 1–α_i, will be $\left[\widetilde{x_i} - \Delta, \widetilde{x_i} + \Delta\right]$, where the quantity xi is distributed according to the normal law with center $\widetilde{x_i}$, and dispersion σ_X^2. Then Δ is determined by the expression:

$$\Delta = t\sqrt{\sigma_x^2 / N}, \tag{2.5}$$

where t is the value according to the Student distribution for K–1 degrees of freedom.

To form metric (weighting) threat factors (**Fig. 2.8**) and their impact on security services, we introduce the following notation: j is a security service for both ICS and CPS. Basic security services: C – confidentiality; I – integrity; A – availability; Au – authenticity, Aff – involvement (affiliation). Thus, a tuple of security services $j = \{C, I, A, Au, Aff\}$ is formed in the classifier; N – the number of threats; K – the number of experts who participated in the expert threat assessment; $\{i\}_1^N$ – current number of the *i*-th threat; $\{k\}_1^K$ – current number of the expert.

To evaluate the hybrid and synergetic components of the impact of modern threats, we use the following sequence of actions:

1*st step.* Determination of the average expert rating for all threats to a particular security service:

$$w_{ICS}^{j}=\frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K}w_{ICSik}^{j},$$

$$w_{CPS}^{j}=\frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K}w_{CPSik}^{j}, \qquad (2.6)$$

where w_{ICSik}^{j} is the value of the metric coefficient set by the k-th expert for the i-th threat of the j-th security service for ICS, w_{ICSik}^{j} is the value of the metric coefficient set by the k-th expert for the i-th threat of the j-th security service for CPS.

2*nd step.* Formation of weighting factors for the threat manifestation conditions for ICS and CPS (**Table 2.10**):

$$\alpha_i^{ICS},\ i\in[0.067;\ 0.133;\ 0.2;\ 0.267;\ 0.333],$$

$$\alpha_i^{CPS},\ i\in[0.067;\ 0.133;\ 0.2;\ 0.267;\ 0.333].$$

Table 2.10 Selection of weights α_i of manifestations of the i-th threat

α_i	**Manifestation conditions**
0.067	The threat does not occur more than once every 5 years
0.133	The threat does not occur more than once a year
0.2	The threat does not occur more than once a month
0.267	The threat does not occur more than once a week
0.333	The threat is daily

3*rd step.* Determining the implementation of each threat for ICS and CPS:

$$w_{ICSi}^{j}P_{ICSi}^{j}=\frac{1}{K}P_{ICSi}^{j}\sum_{k=1}^{N}w_{ICSik}^{j},$$

where

$$P_{ICSi}^{j}\in\left\{\alpha_i^{ICS}\right\},$$

$$w_{CPSi}^{j}P_{CPSi}^{j}=\frac{1}{K}P_{CPSi}^{j}\sum_{k=1}^{N}w_{CPSik}^{j},\quad P_{CPSi}^{j}\in\left\{\alpha_i^{CPS}\right\}.$$

For each security service and *i*-th threat:

– for ICS:

$$w^{I}_{ICSi}\alpha^{C}_{ICSi} = \frac{1}{K}\alpha^{C}_{ICSi}\sum_{k=1}^{K} w^{I}_{ICSik}$$ – confidentiality service,

$$w^{I}_{ICSi}\alpha^{I}_{ICSi} = \frac{1}{K}\alpha^{I}_{ICSi}\sum_{k=1}^{K} w^{I}_{ICSik}$$ – integrity service,

$$w^{A}_{ICSi}\alpha^{A}_{ICSi} = \frac{1}{K}\alpha^{A}_{ICSi}\sum_{k=1}^{K} w^{A}_{ICSik}$$ – availability service,

$$w^{Au}_{ICSi}\alpha^{Au}_{ICSi} = \frac{1}{K}\alpha^{Au}_{ICSi}\sum_{k=1}^{K} w^{Au}_{ICSik}$$ – authenticity service,

$$w^{Aff}_{ICSi}\alpha^{Aff}_{ICSi} = \frac{1}{K}\alpha^{Aff}_{ICSi}\sum_{k=1}^{K} w^{Aff}_{ICSik}$$ – involvement service,

where w^{C}_{ICSi}, w^{I}_{ICSi}, w^{A}_{ICSi}, w^{Au}_{ICSi}, w^{Aff}_{ICSi} are the expert weights of the security services: confidentiality, integrity, availability, authenticity and involvement; α^{C}_{ICSi}, α^{I}_{ICSi}, α^{A}_{ICSi}, α^{Au}_{ICSi}, α^{Aff}_{ICSi} – weighting factor of the security service: confidentiality, integrity, availability, authenticity and authenticity of the manifestation of the *i*-th threat attack;

– for CPS:

$$w^{C}_{CPSi}\alpha^{C}_{CPSi} = \frac{1}{K}\alpha^{C}_{CPSi}\sum_{k=1}^{K} w^{C}_{CPSik}$$ – confidentiality service,

$$w^{I}_{CPSi}\alpha^{I}_{CPSi} = \frac{1}{K}\alpha^{I}_{CPSi}\sum_{k=1}^{K} w^{I}_{CPSik}$$ – integrity service,

$$w^{A}_{CPSi}\alpha^{A}_{CPSi} = \frac{1}{K}\alpha^{A}_{CPSi}\sum_{k=1}^{K} w^{A}_{CPSik}$$ – availability service,

$$w^{Au}_{CPSi}\alpha^{Au}_{CPSi} = \frac{1}{K}\alpha^{Au}_{CPSi}\sum_{k=1}^{K} w^{Au}_{CPSik}$$ – authenticity service,

$$w^{Aff}_{CPSi}\alpha^{Aff}_{CPSi} = \frac{1}{K}\alpha^{Aff}_{CPSi}\sum_{k=1}^{K} w^{Aff}_{CPSik}$$ – involvement service,

where w^{C}_{CPSi}, w^{I}_{CPSi}, w^{A}_{CPSi}, w^{Au}_{CPSi}, w^{Aff}_{CPSi} are the expert weights of the security services: confidentiality, integrity, availability, authenticity and involvement; α^{C}_{CPSi}, α^{I}_{CPSi}, α^{A}_{CPSi}, α^{Au}_{CPSi}, α^{Aff}_{CPSi} – weighting factor of the security service: confidentiality, integrity, availability, authenticity and authenticity of the manifestation of the *i*-th threat attack.

4*th step.* Determining the implementation of several threats to a security service:

$$W^{C}_{ICSsynerg} = \sum_{i=1}^{M} w^{C}_{ICSi}\alpha_i^{ICS\,C} \cup W^{!}_{CPSsynerg} = \sum_{i=1}^{M} w^{C}_{CPSi}\alpha_i^{CPS\,C}$$

– synergetic effect on the confidentiality service;

$$W^{I}_{ICSsynerg} = \sum_{i=1}^{M} w^{I}_{ICSi}\alpha_i^{ICS\,I} \cup W^{I}_{CPSsynerg} = \sum_{i=1}^{M} w^{I}_{CPSi}\alpha_i^{ICS\,I}$$

– synergistic effect on the integrity service,

$$W^{A}_{ICSsynerg} = \sum_{i=1}^{M} w^{A}_{ICSi}\alpha_i^{ICSA} \cup W^{A}_{CPSsynerg} = \sum_{i=1}^{M} w^{A}_{CPSi}\alpha_i^{CPSA}$$

– synergistic effect on the availability service,

$$W^{Au}_{ICSsynerg} = \sum_{i=1}^{M} w^{Au}_{ICSi}\alpha_i^{ICSAu} \cup W^{Au}_{CPSsynerg} = \sum_{i=1}^{M} w^{Au}_{CPSi}\alpha_i^{CPSAu}$$

– synergistic effect on the authenticity service,

$$W^{Aff}_{ICSsynerg} = \sum_{i=1}^{M} w^{Aff}_{ICSi}\alpha_i^{ICSAff} \cup W^{Aff}_{CPSsynerg} = \sum_{i=1}^{M} w^{Aff}_{CPSi}\alpha_i^{CPSAff}$$

– synergistic effect on the involvement service,

where M is the number of several threats that are selected by the expert from the set $\{i\}_i^M$, which is a subset of the entire set of threats of the classifier, that is $M \leq N$.

When forming metric coefficients, it is believed that the results obtained are independent threats, in case of their dependence (coincidence of tuples of threats), it is necessary to use the expression for determining the total probability of dependent events:

$$P(AB) = P(A) + P(B) - P(AB).$$

5*th step.* Determination of the total threat by security components, taking into account the expression (2.6):

$$W^{IS}_{synerg} = \sum_{i=1}^{N} \left(w^{C}_{ICSi} \cap w^{I}_{ICSi} \cap w^{A}_{ICSi} \cap {w_{ICS\,i}}^{Au} \cap {w_{ICS\,i}}^{Aff} \right) \alpha_i^{ICS} \cup$$
$$\cup \sum_{i=1}^{N} \left(w^{C}_{CPSi} \cap w^{I}_{CPSi} \cap w^{A}_{CPSi} \cap w^{Au}_{CPSi} \cap w^{Aff}_{CPSi} \right) \alpha_i^{CPS},$$

$$W^{CS}_{synerg} = \sum_{i=1}^{N} \left(w^{C}_{ICSi} \cap w^{I}_{ICSi} \cap w^{A}_{ICSi} \cap {w_{ICS\,i}}^{Au} \cap {w_{ICS\,i}}^{Aff} \right) \alpha_i^{ICS} \cup$$
$$\cup \sum_{i=1}^{N} \left(w^{C}_{CPSi} \cap w^{I}_{CPSi} \cap w^{A}_{CPSi} \cap w^{Au}_{CPSi} \cap w^{Aff}_{CPSi} \right) \alpha_i^{CPS},$$

$$W^{SI}_{synerg} = \sum_{i=1}^{N} \left(w^{C}_{ICSi} \cap w^{I}_{ICSi} \cap w^{A}_{ICSi} \cap w^{Au}_{ICSi} \cap w^{Aff}_{ICSi} \right) \alpha_i^{ICS} \cup$$
$$\cup \sum_{i=1}^{N} \left(w^{C}_{CPSi} \cap w^{I}_{CPSi} \cap w^{A}_{CPSi} \cap w^{Au}_{CPSi} \cap w^{Aff}_{CPSi} \right) \alpha_i^{CPS}.$$

To determine the generalized synergistic threat:

$$W_{synerg}^{IS,CS,SI} = W_{synerg}^{IS} \cup W_{synerg}^{CS} \cup W_{synerg}^{SI}.$$

To determine the generalized synergistic threat, taking into account its hybridity for ICS:

$$W_{ICSsynerg}^{\text{hybrid}\,C,I,A,Au,Aff} = W_{ICSsynerg}^{C} \cap W_{ICSsynerg}^{I} \cap W_{ICSsynerg}^{A} \cap W_{ICSsynerg}^{Au} \cap W_{ICSsynerg}^{Aff}.$$

To determine the generalized synergistic threat, taking into account its hybridity for CPS:

$$W_{CPSsynerg}^{\text{hybrid}\,C,I,A,Au,Aff} = W_{CPSsynerg}^{C} \cap W_{CPSsynerg}^{I} \cap W_{CPSsynerg}^{A} \cap W_{CPSsynerg}^{Au} \cap W_{CPSsynerg}^{Aff}.$$

To determine the generalized hybrid synergistic threat:

$$W_{synerg}^{\text{hybrid}\,IS,CS,SI} = W_{ICSsynerg}^{\text{hybrid}\,C,I,A,Au,Aff} \cup W_{CPSsynerg}^{\text{hybrid}\,C,I,A,Au,Aff}.$$

6*th step.* Determining the economic costs of preventing an attack.

The introduction of cost indicators of threats allows implementing an algorithm for constructing a rating of potential threats and the importance of information resources to be protected.

The algorithm proposed in [36] implements the following actions. Both sides of the attack are determined by the importance (rating) of the attacks that are economically feasible.

1*st step.* Determination of attacks, the effect of which exceeds the costs of their implementation:

$$Tr_R^A = \left\{ Tr_i \middle| \left(P_i^A - C_i^A\right) > 0 \right\} \forall Tr_i \in Tr, \tag{2.7}$$

where Tr_R^A – a set of the potential threats, the implementation of which is effective for the attacker; Tr_i – threat to the *i*-th information resource; P^A – cost assessment of the success of the attack on the *i*-th resource by the attacker; C^A – the cost of an attack on the *i*-th resource by the attacker.

2*nd step.* Determining the direction of protection, which provides an effect higher than the cost of their provision.

$$Tr_C^D = \left\{ Tr_j \middle| \left(P_i^D - C_i^D\right) > 0 \right\} \forall Tr_j \in Tr, \tag{2.8}$$

where Tr_C^D – a set of the threats against which it is economically feasible to build protection; P_i^D – assessment of the cost of the loss of the *i*-th information resource for the defense; C_i^D – the cost of protecting the *i*-th information resource for the protection side.

3*rd step.* Determination of importance factors for attackers. Defined as a share of the winnings of the total winnings that can be obtained potentially when implementing the entire range of threats to attackers:

$$K_i^A = \frac{P_i^A - C_i^A}{\sum_{i=1}^{M}\left(P_i^A - C_i^A\right)}, \quad \forall Tr_i \in Tr_R^A, M = \left|Tr_R^A\right|, \tag{2.9}$$

where K_i^A is rating coefficient (importance) of the threat to the *i*-th information resource; *M* is the power of a set of selected potentially effective threats to the attacking side.

4*th step.* Determination of importance factors for defenders. Defined as the share of the winnings of the total winnings that can be obtained potentially when implementing the entire range of protective measures:

$$K_j^D = \frac{P_i^D - C_i^D}{\sum_{i=1}^{N}\left(P_i^D - C_i^D\right)}, \quad \forall Tr_j \in Tr_C^D, N = \left|Tr_C^D\right|, \tag{2.10}$$

where K_j^D is the rating coefficient (importance) of building the protection of the *j*-th information resource.

5*th step*. The selection of critical threats based on the evaluation of the product of the importance coefficients of the attacker and the attacker is maximum:

$$Tr_l = \arg\max_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A. \tag{2.11}$$

Thus, the main difference of the proposed approach is the ability to take into account not only the opinion of experts, but also to form an objective assessment and integration of threats, which allows forming their synergistic effect and hybridity. In addition, the use of the ISO model in the classifier allows you to «identify» critical places in the infrastructure not only of cyberphysical systems, but also in synthesis with Internet technologies of cyberspace and «G» technologies. This approach intuitively allows you to focus on the weak points of comprehensive protection, taking into account economic costs in the face of low funding and the «profitability» of an attack by attackers.

2.6 DEVELOPMENT OF THE SPATIO-TEMPORAL STRUCTURE OF THE MODEL BASIS FOR THE CONFLICT-COOPERATIVE INTERACTION OF SECURITY AGENTS

To predict the possible behavior of the attacker, justify the choice of countermeasures at the systemic level of cyber threats and calculate the required amount of investment in cybersecurity with an appropriate distribution of areas and time of investment proposed a concept of modeling the behavior of security agents, which is implemented at three levels (level of security system, level of individual agents, level of group of agents) and is aimed at ensuring the security of business processes of the organization, which allows you to create a contour of business processes of the security system (**Fig. 2.9**).

The following notation was used to formally describe the model basis of the concept of modeling the behavior of security agents.

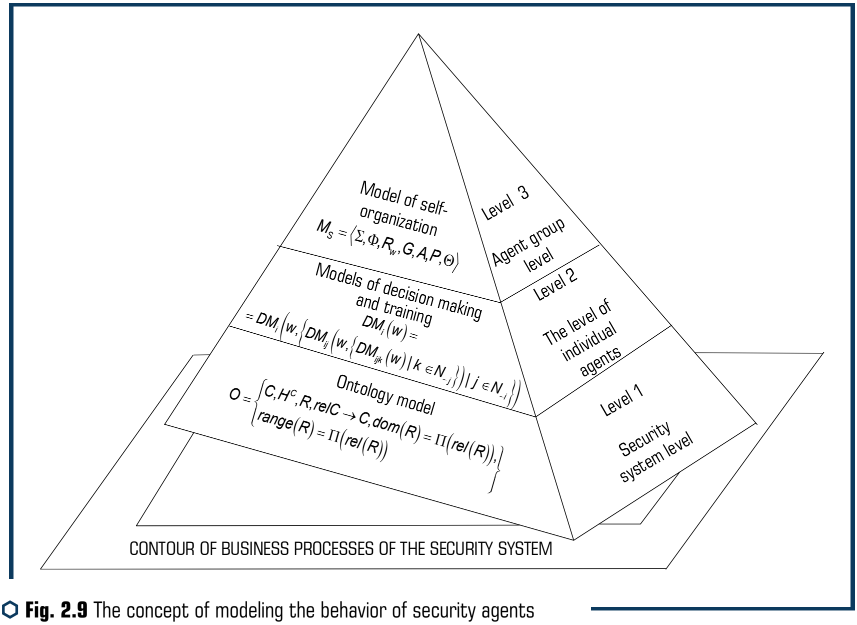

Model of self-organization
$M_S = \langle \Sigma, \Phi, R_w, G, A, P, \Theta \rangle$
Models of decision making and training
$DM_i(w) = DM_i\left(w, \left\{DM_{ij}\left(w, \left\{DM_{ijk}(w) \mid k \in N_{-j}\right\}\right) \mid j \in N_{-i}\right\}\right)$
Ontology model
$O = \left\{ \begin{matrix} C, H^c, R, relC \to C, dom(R) = \Pi(rel(R)), \\ range(R) = \Pi(rel(R)) \end{matrix} \right\}$
Level 3
Agent group level
Level 2
The level of individual agents
Level 1
Security system level
CONTOUR OF BUSINESS PROCESSES OF THE SECURITY SYSTEM

Fig. 2.9 The concept of modeling the behavior of security agents

For the ontology model: C – the set, elements of which are called concepts; H^C – hierarchy of concepts; R – the set, elements of which are called relations; $rel : R \to C \times C$ – a function that correlates concepts not taxonomic; $dom : R \to C$ – function that specifies the subject area R, and $range(R) : \prod_2 (rel(R))$ sets its range.

For the decision-making and training model: w – specific situation; W – the set of all possible situations; DM_i – the decision made by the i-th agent.

For the model of self-organization: Σ – system structure; Φ – system function; R_w – emergence relations; G – set of goals; A – relations of adaptability; P – a set of memory elements; Θ – set of time points.

The following definitions are defined:

– *definition 1*. Critical business processes – processes whose improper organization or non-compliance with the requirements for their implementation may pose an actual or potential threat to product quality and, consequently, to business efficiency;

– *definition 2*. The contour of business processes of the organization – a set of information resources and related business processes, the implementation of which in a given sequence ensures the achievement of the goal of the organization:

$$S^{BC} = \left\{ \left\langle S^{BP_1}, IR^{BP_1}, T^{BP_1} \right\rangle, \ldots, \left\langle S^{BP_n}, IR^{BP_n}, T^{BP_n} \right\rangle \right\}, \tag{2.12}$$

where S^{BP} – business process contour as a set of business processes, each of which represents: S^{Bpi} – i-th business process, defined by the structure of the links of individual business operations that are performed in a certain sequence; IR^{BPi} – a set of information resources of the i-th business process; T^{BPi} – a set of threats affecting the i-th business process;

– *definition 3.* The contour of business processes of the security system – a set of business processes and the resources necessary for them, the implementation of which ensures the proper functioning of the contour of business processes of the organization:

$$S^{BP} = \left\{ \left\langle S^{BP_1}, Rs^{BP_1}, T^{BP_1} \right\rangle, \ldots, \left\langle S^{BP_m}, Rs^{BP_m}, T^{BP_m} \right\rangle \right\}, \tag{2.13}$$

where S^{BP} – security business process contour as a set of business processes, each of which represents; S^{BSi} – i-th business process, defined by the structure of the links of individual business operations that are performed in a certain sequence in the security system; IR^{BSi} – a set of information resources protected by the i-th business process of the security system; T^{BSi} – a set of threats, protection from which provides the i-th business process of the security system.

The security system business process contour combines business processes: security management, ensuring security, implementation, planning, testing and improvement.

At the first level of the Concept, the proposed ontological model is used as a carrier of knowledge about conflict-cooperative interactions of security system agents. The formalized ontology model is proposed as follows:

$$O = \left\{ C, H^C, R, relC \to C, dom(R) = \Pi\left(rel(R)\right), range(R) = \Pi\left(rel(R)\right) \right\}, \tag{2.14}$$

where C – the set, elements of which are called concepts; H^C: H^C – hierarchy of concepts, at $H^C \subseteq C \times C$; R – the set, elements of which are called relations, C and R do not intersect; $rel: R \to C \times C$ – a function that correlates concepts not taxonomic; $dom: R \to C$ – function, with $dom(R) := \Pi_1\left(rel(R)\right)$ sets the subject area R, and $R \to C$ with $range(R): \Pi_2\left(rel(R)\right)$ sets its range. For $rel(R) = \left(C_1, C_2\right)$ write down $R\left(C_1, C_2\right)$; A^O – a set of axioms of the ontology, expressed in the corresponding logical language.

The analysis of the classifier of existing threats, which is proposed in [56], allowed to formulate the relationship between hybridity and synergy of threats depending on their type and direction. The threat classifier introduces a platform of cost indicators of attacks, which allows to assess threats in terms of economic efficiency of their use and counteraction to them. The proposed scale of measuring the value of losses for expert evaluation in the form: {insignificant, low, medium, high, critical}. Let's mark: i – current threat number $\left(\{i\}_1^N\right)$, k – the current number of the expert who performed the assessment $\left(\{k\}_1^K\right)$. The average value of the experts' assessment of the cost of losses for all threats for a certain contour of business processes for defenders, and the cost of the whole set of attacks for attackers can be written as follows:

$$P_k^A = \frac{1}{KM} \sum_{j=1}^{M} \sum_{i=1}^{K} \alpha_j p_{ijk}^A; \quad C_k^A = \frac{1}{KM} \sum_{j=1}^{M} \sum_{i=1}^{K} \alpha_j c_{ijk}^A, \tag{2.15}$$

$$P_k^D = \frac{1}{KM} \sum_{j=1}^{M} \sum_{i=1}^{K} \alpha_j p_{ijk}^D; \quad C_k^D = \frac{1}{KM} \sum_{j=1}^{M} \sum_{i=1}^{K} \alpha_j c_{ijk}^D,$$

where K – number of experts, M – the number of business transactions that may be targeted by the threat, α_j – he criticality ratio of the business process to which the relevant business transaction belongs, p_{ijk} – assessment by the k-th expert of the cost of losses from the i-th threat of the j-th business process (the upper index identifies A – the attacker, D – the defender), c_{ijk} – similarly for the cost of making threats.

At the second level of the Concept the questions of behavior of separate subjects of security system are considered and models of their behavior, namely models of decision-making are constructed $\left(M_R^{DM}\right)$ and training models $\left(M_R^L\right)$:

$$M_R = \left\{M_R^{DM}, M_R^L\right\}.$$

At the third level, the Concepts of the previous level model are used to build models of group behavior, namely models of coordination, adaptation and self-organization: $M_G = \left\{M_G^C, M_G^A, M_G^{SO}\right\}$.

Thus, the concept of modeling the behavior of interacting agents is developed, the basis of which is a three-level structure of modeling the subjects and business processes of the contours of the organization and security system. The proposed concept differs from the existing ones by using a synergetic model of threats in the formation of areas of protection of information resources of the business process contour.

Based on the purpose of the methodology, it should reflect the processes of behavior from two sides. On the one hand, display the processes that are related to the behavior and characteristics of an individual security agent. And on the other hand – the behaviors and processes that arise as a result of the joint functioning of agents. It is necessary to pay attention to modeling the environment of agents, because such an environment is a carrier of system-forming functions that significantly affect the behavior of a party to the conflict and their characteristics.

Within the framework of the proposed concept, a sequence of development of models, methods and algorithms that make it up is formed. The process of building the methodology consists of 4 stages.

Stage 1. Analysis of BP contours and possible attacks on them:

$$S^{BC} = \left\{\left\langle S^{BP_1}, IR^{BP_1}, Tr^{BP_1}\right\rangle, \ldots, \left\langle S^{BP_n}, IR^{BP_n}, Tr^{BP_n}\right\rangle\right\}, \tag{2.16}$$

where S^{BP} – business process contour as a set of business processes, each of which represents: S^{Bpi} – i-th business process. given the structure of the links of individual business transactions that are performed in a certain sequence; IR^{BPi} – a set of information resources of the i-th business process; T^{BPi} – a set of threats affecting the i-th business process.

Stage 2. Development of level models of individual security system agents:

$$M_G = \left\{M_R^B, M_R^L\right\},$$

where M_G – agents group model; M_R^B – model of agents group behavior; M_R^L – agents group training model.

Stage 3. Development of system-wide level models:

$$M_S = \left\{M_S^C, M_S^{SO}\right\},$$

where M_S – system-wide level model; M_S^C – coordination models; M_S^{SO} – model of self-organization.

Stage 4. Development of methods for determining the most likely threats and assessing their cost indicators:

$$Tr_l = \arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A, \tag{2.17}$$

where K_i^A – rating coefficient (importance) of realization of threat to the *i*-th information resource; K_j^D – rating coefficient (importance) of building protection of the *j*-th information resource.

The following is a set of models, methods and algorithms that form a particular level of methodology, with a brief description of the content of this level. It is clear that all the processes that take place in the contours of business processes, the security of which is provided by security agents, are significantly affected by threats that are aimed at disrupting the normal functioning of business processes. Threats are realized through attacks on all components of security, namely, cybersecurity, information security and information security. As a result, the analysis of the contours of business processes as the main purpose of non-directed threats, it is necessary to begin with the analysis of the threats, the set of which with the relevant indicators reflects the classifier. The compliance of the threat classifier with all models, methods and algorithms of the methodology determines and guarantees the effectiveness of the methodology for modeling the behavior of security agents in general. Thus, the analysis of the contour of business processes must begin with the analysis and improvement of the threat classifier. A new platform has been added to the threat classifier to the existing platforms 1–4 – a platform of attacks cost indicators. This allows to assess the threats in terms of economic efficiency of their implementation and counteraction to them. The improved classification of threats to the security of information resources, in contrast to the existing ones, contains indicators of the cost of the threat and countering the threat. The use of an advanced classifier also allows you to assess the likelihood of a threat and develop an effective defense strategy (**Fig. 2.10**). At the level of individual agents, the basic model is a model of a reflexive agent (**Fig. 2.11**).

Marks in **Fig. 2.10** have the following meaning:

– for the ontology model: C – set, the elements of which are called concepts; H^C – hierarchy of concepts; R – set, the elements of which are called relations; $rel: R \to C \times C$ – a function that correlates concepts not taxonomic; $dom: R \to C$ – function that specifies the subject area R, and $range(R): \prod_2(rel(R))$ sets its range;

– for the business process contour model, the labels were described earlier;

– for the threat classifier: i – current threat number $\left(\{i\}_1^N\right)$, k – the current number of the expert who performed the assessment $\left(\{k\}_1^K\right)$; P_k^A, C_k^A – average values of experts' assessment of the probability and cost of carrying out attacks on all threats; P_k^D, C_k^D – similar scores for defenders; K – number of experts, M – the number of business operations that may be targeted, α_j – the criticality ratio of the business process to which the relevant business transaction belongs.

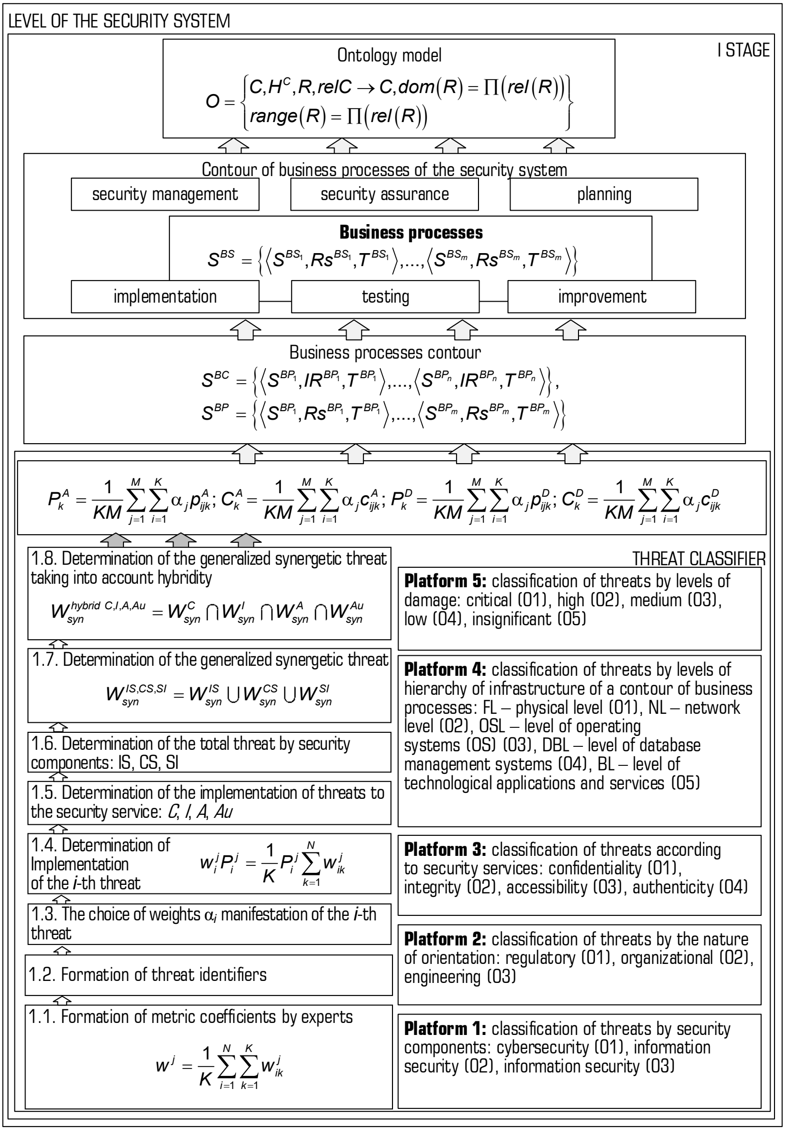

LEVEL OF THE SECURITY SYSTEM
I STAGE
Ontology model
$O = \left\{ \begin{matrix} C, H^C, R, relC \to C, dom(R) = \Pi(rel(R)) \\ range(R) = \Pi(rel(R)) \end{matrix} \right\}$
Contour of business processes of the security system
security management
security assurance
planning
Business processes
$S^{BS} = \{\langle S^{BS_1}, Rs^{BS_1}, T^{BS_1}\rangle, \ldots, \langle S^{BS_m}, Rs^{BS_m}, T^{BS_m}\rangle\}$
implementation
testing
improvement
Business processes contour
$S^{BC} = \{\langle S^{BP_1}, IR^{BP_1}, T^{BP_1}\rangle, \ldots, \langle S^{BP_n}, IR^{BP_n}, T^{BP_n}\rangle\}$,
$S^{BP} = \{\langle S^{BP_1}, Rs^{BP_1}, T^{BP_1}\rangle, \ldots, \langle S^{BP_m}, Rs^{BP_m}, T^{BP_m}\rangle\}$
$P_k^A = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j p_{ijk}^A;\ C_k^A = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j c_{ijk}^A;\ P_k^D = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j p_{ijk}^D;\ C_k^D = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j c_{ijk}^D$
1.8. Determination of the generalized synergetic threat taking into account hybridity
$W_{syn}^{hybrid\ C,I,A,Au} = W_{syn}^C \cap W_{syn}^I \cap W_{syn}^A \cap W_{syn}^{Au}$
1.7. Determination of the generalized synergetic threat
$W_{syn}^{IS,CS,SI} = W_{syn}^{IS} \cup W_{syn}^{CS} \cup W_{syn}^{SI}$
1.6. Determination of the total threat by security components: IS, CS, SI
1.5. Determination of the implementation of threats to the security service: *C*, *I*, *A*, *Au*
1.4. Determination of Implementation of the *i*-th threat
$w_i^j P_i^j = \frac{1}{K} P_i^j \sum_{k=1}^{N} w_{ik}^j$
1.3. The choice of weights α_i manifestation of the *i*-th threat
1.2. Formation of threat identifiers
1.1. Formation of metric coefficients by experts
$w^j = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ik}^j$
THREAT CLASSIFIER
Platform 5: classification of threats by levels of damage: critical (01), high (02), medium (03), low (04), insignificant (05)
Platform 4: classification of threats by levels of hierarchy of infrastructure of a contour of business processes: FL – physical level (01), NL – network level (02), OSL – level of operating systems (OS) (03), DBL – level of database management systems (04), BL – level of technological applications and services (05)
Platform 3: classification of threats according to security services: confidentiality (01), integrity (02), accessibility (03), authenticity (04)
Platform 2: classification of threats by the nature of orientation: regulatory (01), organizational (02), engineering (03)
Platform 1: classification of threats by security components: cybersecurity (01), information security (02), information security (03)

Fig. 2.10 The main components of the I stage of building the methodology (level of security system)

In **Fig. 2.11** the following marks are used: *w* – specific situation; *W* – the set of all possible situations; DM_i – the decision made by the *i*-th agent; a_i – actions of the *i*-th agent; G_i – goals pursued by the *i*-th agent; *e*(*DMi*) – an agent's error when his decision does not meet his purpose;

f_i – agent situation assessment function; *cf* – the function of coordinating the decision of the *i*-th agent with the decision of other agents of the environment; h_i – threat resistance selection function; *ch* – function of coordination of a choice with a choice of other agents.

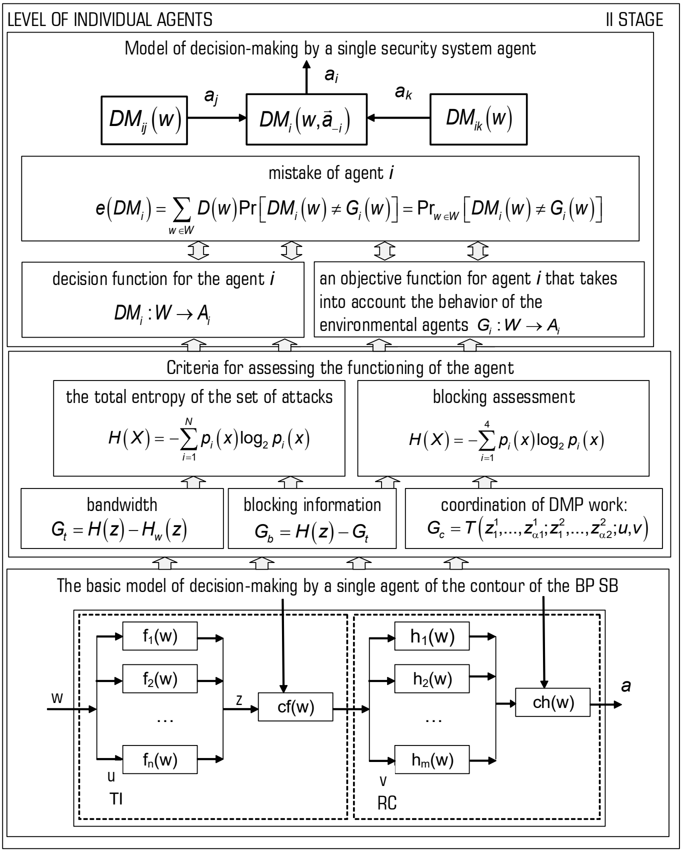

LEVEL OF INDIVIDUAL AGENTS
II STAGE
Model of decision-making by a single security system agent
a_i
a_j
a_k
$DM_{ij}(w)$
$DM_i(w,\bar{a}_{-i})$
$DM_{ik}(w)$
mistake of agent *i*
$e(DM_i)=\sum_{w\in W} D(w)\Pr[DM_i(w)\neq G_i(w)]=\Pr_{w\in W}[DM_i(w)\neq G_i(w)]$
decision function for the agent *i*
$DM_i: W\rightarrow A_i$
an objective function for agent *i* that takes into account the behavior of the environmental agents $G_i: W\rightarrow A_i$
Criteria for assessing the functioning of the agent
the total entropy of the set of attacks
$H(X)=-\sum_{i=1}^{N} p_i(x)\log_2 p_i(x)$
blocking assessment
$H(X)=-\sum_{i=1}^{4} p_i(x)\log_2 p_i(x)$
bandwidth
$G_t=H(z)-H_w(z)$
blocking information
$G_b=H(z)-G_t$
coordination of DMP work:
$G_c=T(z_1^1,\dots,z_{\alpha1}^1;z_1^2,\dots,z_{\alpha2}^2;u,v)$
The basic model of decision-making by a single agent of the contour of the BP SB
w
$f_1(w)$
$f_2(w)$
…
$f_n(w)$
u
TI
z
cf(w)
$h_1(w)$
$h_2(w)$
…
$h_m(w)$
v
RC
ch(w)
a

Fig. 2.11 The main components of the II stage of methodology construction (level of individual agents)

The resulting model of the first level of methodology is a model of the ontology of the relationship between the agents of the parties to the cyber conflict, which can be considered as a carrier of knowledge about the subject area. To build the model, the approach of automated construction of ontology based on various scientific sources (planar texts) TextToOnto was used. The model of ontology of behavior of agents in the conditions of the conflict contains basic concepts of processes of interaction of agents of security systems, and also the concepts reflecting interaction of agents of opposition, instead of technical parties of cyberconflict. This orientation of the ontological model allows to justify the choice of the model of behavior of antagonistic agents in the conditions of hybrid threats.

The main assumption of building a model is the assumption that the decision maker is considered as an information channel. In this case, the main indicators of its functioning can be obtained using information theory. These include bandwidth, generation, blocking and coordination of information. These indicators can be used for both an individual agent and a group of agents.

The basic function of a security agent is the decision function. These decisions can concern both the process of assessing the situation and determining the type of threats, and the definition of countermeasures. The basic model of decision-making proposed at this level by a single agent implements the decision-making process in two stages. Each of these stages (assessment of the situation and the choice of means of counteraction) involves the coordination of the formed assessment with the assessments of other decision-makers. The presence in the dynamic model of behavior of an individual agent of information exchange processes at all stages of decision-making with other cooperating agents in contrast to existing models is a significant difference. Taking into account this feature of decision-making behavior significantly affects the effectiveness of business process protection processes from cyberattack in the conditions of hybrid threats. Such an exchange can be considered as a basis for the formation of scenarios of group behavior.

The second feature of the model is the ability to assign a level of reflection, which allows the opposing party to build a model of possible behavior of the opposing party to the conflict. Thus, a zero level of reflection indicates that the security agent has no information about the agent environment of the confrontation. Whereas the first level of reflection indicates that the agent has an idea of functioning in the environment of other agents. The second level indicates that the opposite side of the conflict is also reflexive, i.e. has a model of behavior of the opposite side, and so on. The recursive model of the reflexive agent contains models of the behavior of the attacker and allows you to model the probable actions of attackers, and thus predict the consequences of decisions made by the defense. Analysis of the reflexive abilities of agents shows that it is impractical to implement reflection above the 2nd level.

The second feature of the model of an individual security agent is the ability to take into account the learning processes in the process of combating cyber threats. The learning processes also reflect the reflexive properties of agents. In traditional learning models, it is possible to accumulate information about changes in the behavior of the opposite side of the conflict and to make predictions about the actions of the opposite side of the conflict. That is, one's own behavior is carried out within the framework of formal decision-making theory as a game against passive nature. And training in the face of the active side of the conflict takes into account that the enemy is an active agent, has its own goals and responds based on their own goals and taking into account the previous actions of the enemy. That is, the opposite side is active and also implements the learning process, ie the choice of reaction should be analyzed on the basis of game theory and taking into account the reflexive abilities of the agent.

Thus, at the level of individual agents, models of training of reflexive agents are proposed, which differ from the models of traditional training in that they take into account the change in the behavior of environmental agents. To assess the quality of training and the dynamics of processes, the use of the following indicators is proposed: the rate of change of agent decisions, the rate of change, the retention rate, and the generalized volatility ratio. The proposed coefficients show how long the agent will adhere to the decision, the agent's willingness to review the previous decision and his ability to respond quickly to changes in the environment of confrontation.

In contrast to the existing ones, the proposed model of agent training takes into account the multi-agent operating environment, which allows to adapt the behavior of the agent in a dynamic environment. In other words, when training, the agent takes into account the fact that he is in the process of confrontation with an active opponent. An active opponent may have his own goals, is characterized by an appropriate level of rationality, and has the ability to learn.

To develop models of the third level of methodology, the model of behavior of an individual agent is modified to take into account the dynamics of processes and interactions of individual agents. That is, the agent's reaction is formed not only under the influence of the obtained results of the situation analysis, but also taking into account similar decisions made by agents of the dynamic environment (**Fig. 2.12**). In Fig. **2.12** the following notation is used:

– $W=\{w_i\}$ – set of confrontation states (information about cyberattacks);
– $A=\{a_i\}$ – the set of actions that an agent can perform;
– $Z=\{z_j\}$ – the set of states in which the agent may be;
– $z_i(t+1)=f_i(z_i(t),u_i(t),w_i(t))$ – transition function;
– $u_{ij}(t)=g_{ij}(z_i(t))$ – aggregation function;
– $a_i(t)=h_i(z_i(t),u_{ji}(t))$ – local output function;
– $C=c_i(z_i(t),z_i(t+1),u_i(t),w_i(t))$ – local cost function.

The level of the agent group should include various methods of coordination in the security agent groups. Different methods of coordinating the behavior of agents are explained by the fact that the method takes into account the level of reflexivity of the agent. Thus, the method of coordination without communication reflects the fact that the agent has the 0th level of reflexivity, i.e. it is an agent that in no way takes into account the functioning of such agents. When the agent builds a model of the opponent's behavior, which in turn is also my model of the opponent's behavior. The use of different methods of coordination allows to organize cooperation between security agents to ensure the tasks of cyber security in a fairly wide range of operating conditions.

The application of the proposed characteristics to assess the effectiveness of the functioning of agents can be demonstrated by the example of two structures of interaction of agents. The first structure is parallel, when agents work together, possibly independently, coordinating their actions independently.

In the second structure, one of the agents coordinates the work of the other two agents. Knowledge of the specific characteristics of agents, in particular their effectiveness in making decisions and coordinating work, will allow to make a conclusion which of the structures is more effective in terms of productivity of a group of agents.

The method of assessing the effectiveness of the structure of interaction of a group of security agents allows to justify the choice of the structure of interaction, as well as to distribute the functions of protection of business process resources, which provides increased security of the business process. In contrast to the existing ones, the proposed method considers the agent as a processor of information with appropriate characteristics and is based on information processing processes and relevant characteristics of the effectiveness of the security system.

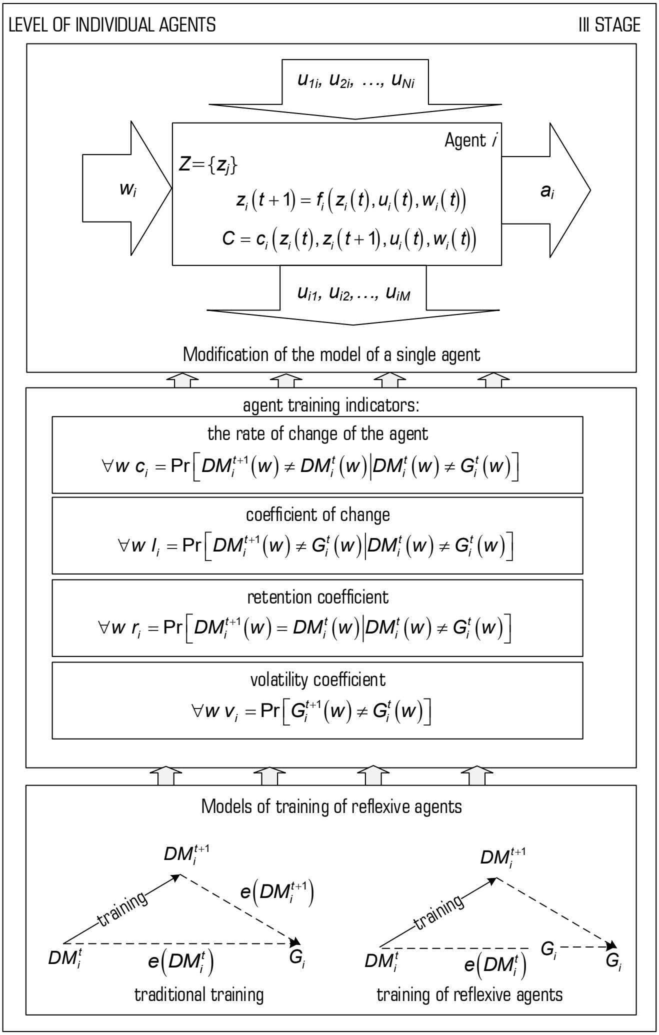

LEVEL OF INDIVIDUAL AGENTS
III STAGE
$u_{1i}, u_{2i}, \ldots, u_{Ni}$
Agent i
$Z=\{z_j\}$
w_i
$z_i(t+1)=f_i(z_i(t),u_i(t),w_i(t))$
$C=c_i(z_i(t),z_i(t+1),u_i(t),w_i(t))$
a_i
$u_{i1}, u_{i2}, \ldots, u_{iM}$
Modification of the model of a single agent
agent training indicators:
the rate of change of the agent
$\forall w\ c_i=\Pr\left[DM_i^{t+1}(w)\neq DM_i^t(w)\middle|DM_i^t(w)\neq G_i^t(w)\right]$
coefficient of change
$\forall w\ l_i=\Pr\left[DM_i^{t+1}(w)\neq G_i^t(w)\middle|DM_i^t(w)\neq G_i^t(w)\right]$
retention coefficient
$\forall w\ r_i=\Pr\left[DM_i^{t+1}(w)=DM_i^t(w)\middle|DM_i^t(w)\neq G_i^t(w)\right]$
volatility coefficient
$\forall w\ v_i=\Pr\left[G_i^{t+1}(w)\neq G_i^t(w)\right]$
Models of training of reflexive agents
DM_i^{t+1}
training
$e(DM_i^{t+1})$
DM_i^t
$e(DM_i^t)$
G_i
traditional training
DM_i^{t+1}
training
DM_i^t
$e(DM_i^t)$
G_i
G_i
training of reflexive agents

Fig. 2.12 The main components of the III stage of methodology construction (level of individual agents)

The final model of self-organization combines models of the structure and functions of the security system, the relationship of emergence and adaptability, as well as sets such as sets of goals, memory elements, moments of time and input influences. The self-organization model provides the construction of a robust security system in the conditions of synergetic and hybrid threats, is based on the synergy of advanced models, and provides the emergent properties of business processes in the security loop. The ability to aggregate models that focus on hybrid and synergistic threats, significantly distinguishes it from known similar models (**Fig. 2.13**).

In **Fig. 2.13** for the model of self-organization used the following notation: Σ – system structure; Φ – system function; R_w – relations of emergence; G – set of goals; A – adaptive relations; P – a set of memory elements; Θ – set of time points.

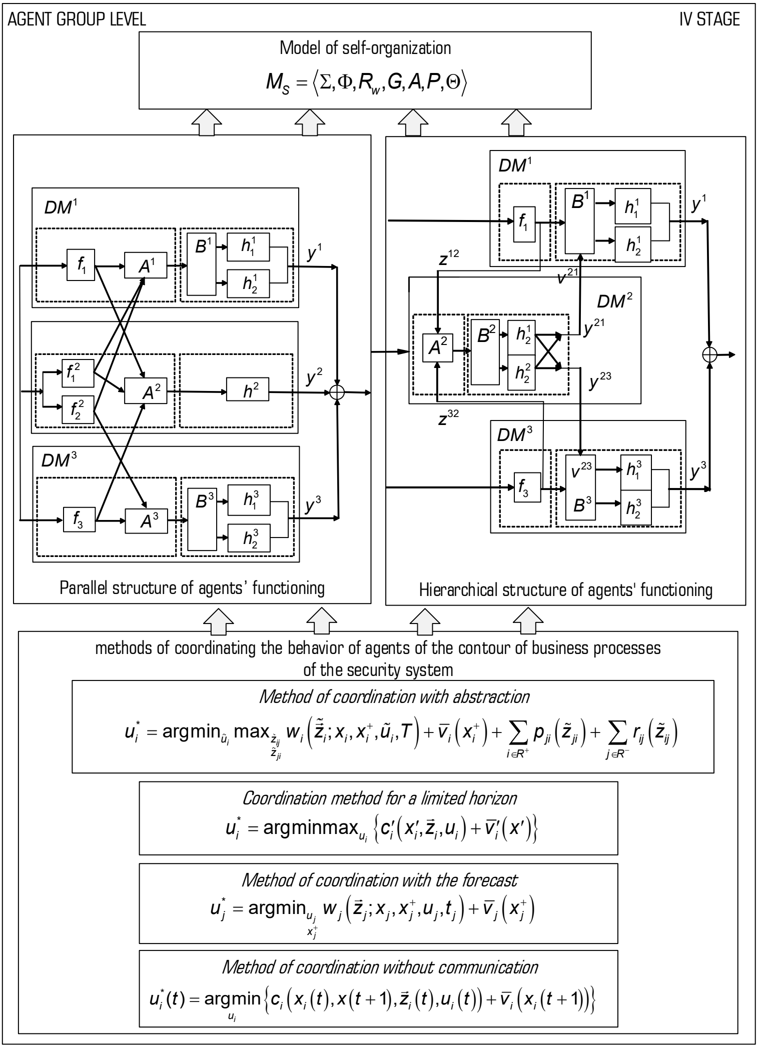

AGENT GROUP LEVEL
IV STAGE
Model of self-organization
$M_S = \langle \Sigma, \Phi, R_w, G, A, P, \Theta \rangle$
DM^1
f_1
A^1
B^1
h_1^1
h_2^1
y^1
f_1^2
f_2^2
A^2
h^2
y^2
DM^3
f_3
A^3
B^3
h_1^3
h_2^3
y^3
Parallel structure of agents' functioning
DM^1
f_1
B^1
h_1^1
h_2^1
y^1
z^{12}
v^{21}
DM^2
A^2
B^2
h_2^1
h_2^2
y^{21}
y^{23}
z^{32}
DM^3
f_3
v^{23}
B^3
h_1^3
h_2^3
y^3
Hierarchical structure of agents' functioning
methods of coordinating the behavior of agents of the contour of business processes of the security system
Method of coordination with abstraction
$u_i^* = \operatorname{argmin}_{\hat{u}_i} \max_{\substack{\tilde{z}_{ij} \\ \hat{\tilde{z}}_{ji}}} w_i\left(\tilde{\vec{z}}_i; x_i, x_i^+, \tilde{u}_i, T\right) + \bar{v}_i\left(x_i^+\right) + \sum_{i \in R^+} p_{ji}\left(\tilde{z}_{ji}\right) + \sum_{j \in R^-} r_{ij}\left(\tilde{z}_{ij}\right)$
Coordination method for a limited horizon
$u_i^* = \operatorname{argminmax}_{u_i} \left\{ c_i'\left(x_i', \vec{z}_i, u_i\right) + \bar{v}_i'\left(x'\right) \right\}$
Method of coordination with the forecast
$u_j^* = \operatorname{argmin}_{\substack{u_j \\ x_j^+}} w_j\left(\vec{z}_j; x_j, x_j^+, u_j, t_j\right) + \bar{v}_j\left(x_j^+\right)$
Method of coordination without communication
$u_i^*(t) = \operatorname*{argmin}_{u_i} \left\{ c_i\left(x_i(t), x(t+1), \vec{z}_i(t), u_i(t)\right) + \bar{v}_i\left(x_i(t+1)\right) \right\}$

Fig. 2.13 The main components of the IV stage of methodology construction (agent group level)

The main purpose of developing a methodology for modeling the behavior of agents is to increase the level of security of the business process of the organization. This is done by obtaining an estimate of the likelihood of an attack on business processes and information resources that ensure their functioning. The proposed algorithm for assessing the economic effectiveness of the threat and countering them allows you to identify the most likely threats aimed at violating the security of information resources.

As a result, economically justify the distribution of limited funds between different information resources and business processes that require protection. The proposed algorithm for determining the most likely threat allows to organize an effective allocation of limited funds to protect the resources of the contour of business processes. This is done on the basis of using the results of modeling the behavior of cooperative-antagonistic agents, to determine and assess the likelihood of a threat.

The model of determining the most probable threat allows to organize an effective allocation of limited funds to protect the resources of the contour of business processes based on the results of modeling the behavior of cooperative antagonistic agents to determine and calculate the probability of threat. The proposed evaluation algorithm takes into account possible decisions on the attack and counteraction to it, made by all parties to the cyber conflict in terms of synergy and hybrid threats. That is, taking into account the decisions of all parties to the conflict, which have reflexive properties and reflect the cost of resources to be protected, and the cost of the attack, is a significant difference between the proposed algorithm.

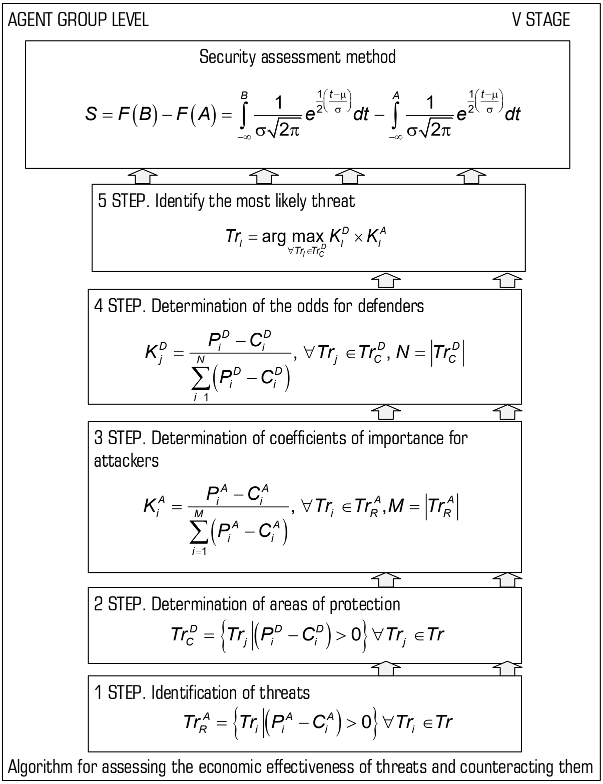
As a result, the algorithm allows you to identify the range of resources that are most likely to carry out cyberattacks (**Fig. 2.14**).

A graphical representation of the levels of representation of models, methods and algorithms as components of the methodology for modeling the behavior of agents is shown in **Fig. 2.15**.

The safety assessment method is based on the assumption that the safety assessment is described by Gaussian law.

Notation in **Fig. 2.14** have the following meaning: Tr_R^A – set of potential threats, the implementation of which is effective for the attacker; Tr_i – threat to the *i*-th information resource; P_i^A – assessment of the cost of success of the attack on the *i*-th resource of the business process by the attacker; C_i^A – the cost of an attack on the *i*-th resource of the business process by the attacker; Tr_C^D – set of threats against which it is advisable to protect in terms of value; P_i^D – assessment of the cost of loss of the *i*-th information resource for the defense party; C_i^D – the cost of protection of the *i*-th information resource for the defense party; K_i^A – rating coefficient (importance) of realization of threat to the *i*-th information resource; M – power of a set of selected potentially effective threats to the attacking party; K_j^D – rating coefficient (importance) of building protection of the *j*-th information resource.

Thus, the proposed methodology for modeling the behavior of interacting agents, the basis of which is a three-level structure of modeling entities and business processes of security systems and organizations, increases the level of security of business processes by reducing 1.76 times the number of hybrid threats, which reduces losses by 1.65 times and increases the time of choice of means of resistance by reducing by 38 % the time to identify the threat online.



AGENT GROUP LEVEL

V STAGE

Security assessment method

$$S = F(B) - F(A) = \int_{-\infty}^{B} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)} dt - \int_{-\infty}^{A} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)} dt$$

5 STEP. Identify the most likely threat

$$Tr_l = \arg\max_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A$$

4 STEP. Determination of the odds for defenders

$$K_j^D = \frac{P_i^D - C_i^D}{\sum_{i=1}^{N}\left(P_i^D - C_i^D\right)}, \forall Tr_j \in Tr_C^D, N = \left|Tr_C^D\right|$$

3 STEP. Determination of coefficients of importance for attackers

$$K_i^A = \frac{P_i^A - C_i^A}{\sum_{i=1}^{M}\left(P_i^A - C_i^A\right)}, \forall Tr_i \in Tr_R^A, M = \left|Tr_R^A\right|$$

2 STEP. Determination of areas of protection

$$Tr_C^D = \left\{Tr_j \middle| \left(P_i^D - C_i^D\right) > 0\right\} \forall Tr_j \in Tr$$

1 STEP. Identification of threats

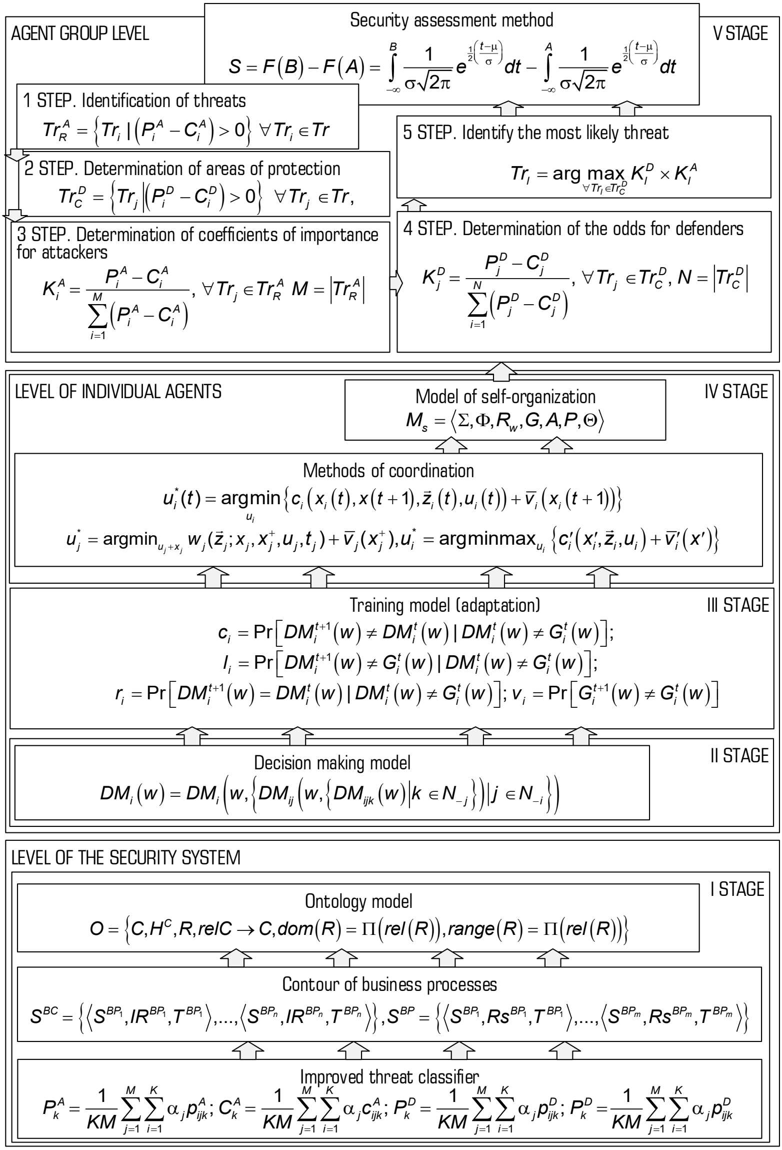
$$Tr_R^A = \left\{Tr_i \middle| \left(P_i^A - C_i^A\right) > 0\right\} \forall Tr_i \in Tr$$

Algorithm for assessing the economic effectiveness of threats and counteracting them

⬡ **Fig. 2.14** The main components of the V stage of methodology construction (level of group of agents)

The combined use of mathematical modeling methods, the theory of adaptation and artificial intelligence methods (training, pattern recognition and problem-solving planning) with the corresponding creation of ontologies of cybersecurity systems that ensure the filling of databases, models and knowledge will allow you to implement an effective adaptive decision support system that will be useful a tool for managers at any level at all stages of decision making and implementation. The presented approaches can be used as a basis for building and operating decision support systems, increasing the area of application of such systems due to the formation of their adaptability properties.

The proposed methodology is based on the combined use of all the above set of models, methods and algorithms. It can be argued that the combined use of models, methods and algorithms leads to a synergistic effect in the modeling process. The methodology allows to predict the possible behavior of the attacker, to justify the choice of countermeasures at the system level of cyber threats and to calculate the required amount of investment in cybersecurity with an appropriate distribution of security components and investment time.


AGENT GROUP LEVEL
Security assessment method
$S = F(B) - F(A) = \int_{-\infty}^{B} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)} dt - \int_{-\infty}^{A} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)} dt$
V STAGE
1 STEP. Identification of threats
$Tr_R^A = \{Tr_i \mid (P_i^A - C_i^A) > 0\} \ \forall Tr_i \in Tr$
2 STEP. Determination of areas of protection
$Tr_C^D = \{Tr_j \mid (P_i^D - C_i^D) > 0\} \ \forall Tr_j \in Tr,$
3 STEP. Determination of coefficients of importance for attackers
$K_i^A = \frac{P_i^A - C_i^A}{\sum_{i=1}^{M} (P_i^A - C_i^A)}, \ \forall Tr_j \in Tr_R^A \ M = |Tr_R^A|$
4 STEP. Determination of the odds for defenders
$K_j^D = \frac{P_j^D - C_j^D}{\sum_{i=1}^{N} (P_j^D - C_j^D)}, \ \forall Tr_j \in Tr_C^D, \ N = |Tr_C^D|$
5 STEP. Identify the most likely threat
$Tr_l = \arg\max_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A$
LEVEL OF INDIVIDUAL AGENTS
Model of self-organization
$M_s = \langle \Sigma, \Phi, R_w, G, A, P, \Theta \rangle$
IV STAGE
Methods of coordination
$u_i^*(t) = \underset{u_i}{\operatorname{argmin}} \{c_i(x_i(t), x(t+1), \vec{z}_i(t), u_i(t)) + \bar{v}_i(x_i(t+1))\}$
$u_j^* = \operatorname{argmin}_{u_j + x_j} w_j(\vec{z}_j; x_j, x_j^+, u_j, t_j) + \bar{v}_j(x_j^+), u_i^* = \operatorname{argminmax}_{u_i} \{c_i'(x_i', \vec{z}_i, u_i) + \bar{v}_i'(x')\}$
Training model (adaptation)
III STAGE
$c_i = \Pr[DM_i^{t+1}(w) \neq DM_i^t(w) \mid DM_i^t(w) \neq G_i^t(w)];$
$l_i = \Pr[DM_i^{t+1}(w) \neq G_i^t(w) \mid DM_i^t(w) \neq G_i^t(w)];$
$r_i = \Pr[DM_i^{t+1}(w) = DM_i^t(w) \mid DM_i^t(w) \neq G_i^t(w)]; \ v_i = \Pr[G_i^{t+1}(w) \neq G_i^t(w)]$
Decision making model
II STAGE
$DM_i(w) = DM_i\left(w, \left\{DM_{ij}\left(w, \left\{DM_{ijk}(w) \middle| k \in N_{-j}\right\}\right) \middle| j \in N_{-i}\right\}\right)$
LEVEL OF THE SECURITY SYSTEM
I STAGE
Ontology model
$O = \{C, H^C, R, relC \rightarrow C, dom(R) = \Pi(rel(R)), range(R) = \Pi(rel(R))\}$
Contour of business processes
$S^{BC} = \{\langle S^{BP_1}, IR^{BP_1}, T^{BP_1} \rangle, \ldots, \langle S^{BP_n}, IR^{BP_n}, T^{BP_n} \rangle\}, S^{BP} = \{\langle S^{BP_1}, Rs^{BP_1}, T^{BP_1} \rangle, \ldots, \langle S^{BP_m}, Rs^{BP_m}, T^{BP_m} \rangle\}$
Improved threat classifier
$P_k^A = \frac{1}{KM} \sum_{j=1}^{M} \sum_{i=1}^{K} \alpha_j p_{ijk}^A; \ C_k^A = \frac{1}{KM} \sum_{j=1}^{M} \sum_{i=1}^{K} \alpha_j c_{ijk}^A; \ P_k^D = \frac{1}{KM} \sum_{j=1}^{M} \sum_{i=1}^{K} \alpha_j p_{ijk}^D; \ P_k^D = \frac{1}{KM} \sum_{j=1}^{M} \sum_{i=1}^{K} \alpha_j p_{ijk}^D$

⬡ **Fig. 2.15** Spatial-temporal structure of the methodology for modeling the behavior of interacting agents

The effectiveness of the proposed methodology should be supported by the implementation of the following principles:

1. The principle of continuous monitoring of compliance with cybersecurity requirements.

2. The principle of reproduction and evidence of information about the level of cybersecurity at the protected object.

3. The principle of systemic management of the functioning of the cybersecurity system of the protected object.

4. The principle of preventive measures of cybersecurity.

5. The principle of synergetic elements.

Summarizing, we can state that the synergy of cybersecurity is actually a real requirement of practice, since This property of systems, which gives a multiplier effect, is especially important in the context of a time limit, and if cyber attacks are detected and prevented at the initial stage, this by orders of magnitude reduces the levels of all types of risks of the functioning of the business processes of the protected organization.

3 MATHEMATICAL MODELS OF INFORMATION PROTECTION IN SOCIAL NETWORKS, TAKING INTO ACCOUNT THE SPECIFICS OF THEIR PARAMETERS

ABSTRACT

The development of mathematical models for assessing the stability of the information protection system in social networks, which is based on the analysis of the parameters of the protection system. The models allow to study the parameters of system protection and realize the necessary actions to improve the information protection system, taking into account the nonlinear interaction of the elements of the protection system and external influences. The proposed mathematical model of the information protection system in social networks in contrast to the existing ones, allows an objective assessment of the equilibrium between information security threats and specific parameters of the social network, such as information dissemination, network expansion and correlation coefficient. The improved mathematical model and method of increasing the level of information security, in contrast to the existing ones, takes into account the impact on the information security system of trust, reputation, correlation and clustering coefficient of the network. The application of the model and methodology allows analyzing the impact on the information protection system of other situational parameters.

KEYWORDS

Social networks, trust, reputation, protection factor, correlation.

In today's world, information needs reliable protection: from unauthorized access and distribution, accidental deletion or alteration. All developed European countries are concerned about the problem of information security, as well as the protection of personal data of citizens [105–107]. This is due to the fact that informatization and digitization of information have become widespread in all areas of human activity, including the storage of personal and work data.

Mass production, implementation and operation of information systems have led to a range of new problems in the field of personal security and security of society and the state. Attention to these problems is natural [106, 107]. If a commercial organization allows the leakage of more than 20 % of important internal information, it goes bankrupt in 60 cases out of 100 [108–116]. Analysis of statistics shows [115, 117] that 93 % of companies that left free access to their own confidential information for more than 10 days, left the business. At the same time, half of them declared their failure immediately.

The need for information security is due to the fact that there are many entities and structures that are very interested in other people's information and willing to pay a high price for it. Thus, the cost of eavesdropping devices sold in the United States alone averages about $ 900 million per year [108]. The total damage suffered by the auditioned organizations is about

$ 8 billion annually in the United States. But there are exist and, accordingly, purchased devices for unauthorized access to digital information and intrusion into information systems, interception and decryption of messages, etc. As a result, according to SANS Institute, in the US the average amount of damage from one attack on a corporate system for banking and IT sectors of the economy is about half a million dollars [118–121]. The approximate structure of the consequences of inefficient information security in American organizations from the total annual damage is as follows [117–119]:

– theft of confidential information – 20÷25 %;

– falsification of financial information – 21÷25 %;

– infection with malicious programs – 11÷12 %;

– violation of access to Web-sites – 1÷11 %;

– failure of the information system – 4÷10 %;

– illegal access of employees to information – 4÷9 %;

– other types of damage – 14÷33 %.

Social networks are one of the main methods of communication, connection search and exchange of both public and confidential information. The share of social networks among general networks is constantly growing. The network itself acquires new properties, acting as an independent factor.

Because the information in the global network exists outside of space and time, the network itself becomes an active agent of human influence, keeping, above all, large amounts of data publicly available. In recent years, the vision of the problem of cybersecurity has begun to change significantly, as not only the financial and economic interests and capabilities of human continue to be the subject of cybercrime, but the human itself is increasingly becoming the object of cybercrime.

This problem is especially exacerbated with the strengthening of the digital humanistic nature of education and the growing role of social networks in human life in general.

The protection of personal data in today's information life is perhaps the most important aspect in meeting the safe use of all the capabilities of current technologies. Therefore, the problem of studying the parameters of social networks for their further use in solving problems of information protection and personal data is very relevant.

3.1 SPECIFIC PARAMETERS OF SOCIAL NETWORKS AND THEIR IMPACT ON THE SECURITY OF USER INFORMATION

The exchange of personal data, potentially, allows the use of social networks to solve a wide range of information problems, but there is a problem of data protection. Therefore, the issue of developing new mathematical models for assessing the dependence of personal data protection on trust and the amount of information on social networks is very relevant.

What is **trust** – is a complex mental relationship (positions) [108]. The trust of the cognitive user *X* (his mental state), which characterizes his thinking, in relation to the chosen essence (user *Y*) about the expected behavior (action) α, which is important for achieving goal *G* (specific state of events necessary and desirable for the user *X*). User *X* essentially delegates actions α to user *Y*. What are the mental components of user *X*'s trust in user *Y*? These are the following beliefs:

– **belief in competence:** user *X* must believe that user *Y* can indeed complete the task and produce the expected result needed to achieve goal *G*;

– **belief in intention** (disposition): user *Y* can not only able to perform the task, but also will perform it.

Moreover, belief in intention is formed on the basis of five other beliefs [108]:

– **belief in readiness** (willingness): user *X* believes (simulates the thinking of user *Y*) that user *Y* has decided and intends to perform action α;

– **belief in sustainability** (persistence): user *X* believes that user *Y* is stable in his intentions to take action α if user *Y* is predictable and has no disagreement about the action of α;

– **belief in addiction** (dependence): user *X* believes that user *Y* is necessary to perform the task (strict dependence) or that it is better to rely on it than not to rely (weak dependence);

– **belief in self-confidence**: user *X* must believe that user *Y* knows that he can do the action α. It's hard to trust someone who doesn't trust themselves. Finally, the last component of trust that comes from others;

– **belief in fulfillment** (fulfillment): user *X* believes that goal *G* will be achieved (thanks to user *Y*), so he does not give up goal *G*, does not look for an alternative to user *Y* and achieves goal *G* through user *Y*.

Let's define types of trust [9]:

– provision trust: describes trust when a person trusts a party to provide quality services by a service or resource provider (what we are considering);

– delegation trust: describes the trust in the user (representative) acting and making decisions on behalf of the party he trusts;

– access trust, as a special case of provision trust: describes the provider's trust in agents who are granted access to resources. This is access control;

– trust in authenticity: describes the belief in the claimed authenticity of the user. Used in authentication systems [110];

– contextual trust describes the participant's degree of faith in the necessary systems and institutional mechanisms that support transactions and ensure network security [119] in the event that something goes wrong (insurance, legal system, law enforcement – also considered as a situational context of trust).

Each type of trust uses its own methods to protect the system from malicious users. Strict security mechanisms are used for trust authenticity and trust access [112]:

– communication channel encryption;

– cryptographic authentication and authorization schemes;

– policies for empowerment;

– digital signatures and certificates issued by a trusted third party (the trust transitivity property can be used), etc.

These traditional security practices will not be discussed further. In our further study, we will limit ourselves to examining trust in service delivery and trust delegation (although all of the above types of trust are, of course, interrelated) and methods of protection in online systems.

Soft security mechanisms are used for trust in the provision of services and trust in delegation [113]. Service providers may provide inaccurate information, and traditional security mechanisms cannot protect users from this type of threat. Trust and reputation systems can protect the user from such threats, moreover, they can protect the system itself (so-called Trusted systems). According to the type of trust, the subject of trust is determined: what is the focus of the trust of the subject (the area of the relationship of trust). For example, user *Y* is a «first-class programmer» and can therefore be entrusted with writing a program (provision trust).

Consider the following concepts that we will use in our study.

Actions. Actually, the actions taken by agents in transactions, based on trust in partners (different kinds of entities). For example: «Buy a laptop», «Accept information», etc.

Feedback. After completing the transaction (interaction), agents can evaluate each other's actions (feedback) [10]. Appropriate measures are used for this purpose, the values of which are used to calculate reputation and trust.

We can measure trust through different types of measures. The semantics of measures can be described in terms of specificity-commonality (specific aspect of trust – the average of all aspects) and subjectivity-objectivity (subjective opinion – objective assessment by formal criteria). Subjective and specific measures are used in questionnaires in which people express their opinion on specific things («Please rate the work of site X» on the rating scale «Terrible, Bad, Average, Good, Excellent»), thus forming subjective vector of trust.

The problem with subjective and general measures is that they do not allow some aspects to be assessed. For example, the customer gave a low rating in the transaction because he did not receive the goods on time, but in fact the delivery service was to blame.

Objective and specific measures are used, for example, in technical tests of the product, where the quality of the product is measured objectively (for example, on energy consumption, noise, etc.). Objective and general measures can be an example of calculations on the vector of objective and specific measures. And then there is a repetition of the cycle. Feedback affects trust, trust affects the user's actions in the next transaction, and so on. (We can apply the scheme: reputation, trust, «reciprocity», trust, benefit).

Methods of calculating confidence (computational models), the combination of sources of confidence signals, signaling, the collection of such signals and storage, risk assessment and decision making, as well as the manipulation of such systems are the subject of many studies [11].

Degree of trust – is a subjective confidence of beliefs, quantitative assessment depends on the quantitative assessment of components. When modeling aspects of trust, there is a need to take into account the factors (effects) that occur in social networks [9]:

– reliability. Willingness to rely, delegate performance;

– discretion. Not the monotony of trust (it is natural for a person to divide it into discrete levels);

– subjectivity (personal trust) and asymmetry (if we trust someone, it does not mean that we are also trusted);

– transitivity of trust (in the general case it is not transitive);

– uncertainty of trust (it is difficult to clearly define trust, you can specify boundaries);

– multifactorial (trust consists of many cognitive components: competence, etc.);

– dependence on the context (circumstances and area of trust);

– dependence on recommendations and reputation;

– connection with the concept of reciprocity («eye for an eye»);

– dynamics (trust may change over time with or without experience);

– trust is directly related to risk (vulnerability) and is taken into account when making a decision;

– trust can be based on a history of interactions.

Separately, we will briefly consider the transitivity of trust, social networks and trust-related concepts of risk, risk threshold and decision-making.

Transitivity of trust. In the general case, trust is not transitive [117, 119]. We don't have to trust those, who are trusted by ones that we trust: user *A* trusts user *B*, user *B* trusts user *C*, but user *A* has every right not to trust user *C* (or if user *A* doesn't trust user *B*, and user *B* does not trust user *C*, this does not mean that user *A* does not trust user *C*). But under certain conditions, trust can operate in a chain (has a length limit). At the very least, a previously unknown person recommended to us by someone we trust will be trusted more than a stranger (for example, someone can trust a writer through a publisher, and a publisher can only be trusted because someone recommended him). The context of trust is important here, and we look at trust in terms of reliability.

Social networking users come together to process information effectively, including to share information about trust and reputation. Users form so-called trust networks [12].

Risk, risk threshold and decision making. As already mentioned, the user usually determines the degree of trust, assesses the risk, and on its basis and on the basis of personal risk thresholds determines the decision about the possibility of interaction with a potential partner [109]. The user must trust (even if there is uncertainty of trust) and accept some probability of failure, i.e., take the risk. Risk determines the possible negative consequences of a decision. It is not enough to make some positive assessment of confidence; you need to assess the threshold of «acceptable» damage. The cost of losses can be too high for the user, even regardless of the probability of failure (perhaps very low) and the benefit (perhaps very large) if successful. That is, the danger is too high.

In addition, it should be noted that trust can be irrational, unreasonable assessments of the components of trust [118].

Representation of trust. The value of trust is determined by:

1. Domain. Values can be binary («trust»/»distrust»), discrete (labels denoting the set of natural numbers, natural for human understanding) and continuous (well supported by known mathematical theories, depending on the semantics of values of trust). Noteworthy is the idea of meaning with the semantics of «do not know» and «do not trust». Thus, in some models with a continuous domain, the trust value of the value «I do not trust»: [0; 1], where 0 is «I do not know», and 1 – I trust completely; in others 0 means complete distrust, 0.5 – «I do not know», 1 – complete trust; in the third there is a range [–1; 1], etc.

2. Dimensionality. Some models represent trust by one value and others by several (for example, $<b, d, u>$ – trust value, distrust value, uncertainty value or interval confidence representation). A trustworthy measure of reputation/trust reliability needs to be considered separately (sometimes it is necessary to know how reliably the value of trust/reputation is obtained for a final decision).

3. Semantics. In some models, the value of trust is represented by rating (directly indicates the degree of reliability, for example, «very reliable»), in others – rank (relative value, does not

indicate directly, is the basis for comparison), probability (expectation), faith (belief), fuzzy meaning. This also includes related issues of presenting the history of interactions, policies of trust, protocols of interaction, etc. in the form of rules, records, ontologies (Semantic Web).

Calculation of trust. Trust can be quantified in different ways. Some approaches, including the Semantic Web, use discrete values of trust (eg, trust, distrust, or neutrality), while others use a continuous range [121]. Algorithms for calculations can vary from a simple average value to the calculation of eigenvalues by adjacency matrices of the corresponding graph. Many approaches do not take into account the change in trust over time. In cases where a lot of information is required to calculate the trust or the information is constantly changing, it is usually suggested to use a local trust calculation instead of a global one. The following factors determine the differences between computational models [108].

Conceptual model. Computational models simulate trust either from a cognitive point of view as a function of fundamental beliefs (as a result of the user's mental state), or from a theoretical-game point of view as a subjective probability (as a result of pragmatic play).

Consider the theoretical-game approach [112]. In the social network there is a repetition of the *N* users' game, each of which has uncertainty about the usefulness structures of other users. At each step, the user must simulate the actions of other users (based on their expectations of their actions), maximizing their utility functions. To solve the game, the concept of Nash equilibrium is used, in which one-sided deviation is not beneficial to any of the users. It should be borne in mind that when an agent chooses certain actions, the expectations of other players may change and his reputation will change accordingly (feedback). Therefore, the behavior of users will change in the next stages of the game («tooth for tooth»), which will lead to a new balance.

Disadvantages of this approach:

– players who play over a long period of time are considered (and in large online communities, multiple interactions between players are rare – but can probably be used in narrow professional thematic communities);

– people are limited rational;

– interactions of some users are considered separately from other interactions;

– problems of reputation mechanisms are practically not taken into account;

– information of trust and reputation for probability with increasing complexity of the model is insufficient.

Sources of information for calculating reputation, trust. To calculate the reputation, trust is used as traditional sources: direct experience and indirect information (from witnesses), and less common, for example, information related to the social aspects of user behavior [106]. The right combination of these sources can increase the reliability and accuracy of the calculated value of trust/reputation, although it increases the complexity of the model and requires smart users to process the information provided.

Direct experience. The most reliable source of information. Includes both experiences gained in direct interaction with a partner and experience based on observing the interactions of other users (rarely used in modern models, within the system scenario).

Indirect information (from witnesses). Witness information (so-called word-of-mouth information or indirect information). Although such information is often used, it is more difficult to use in models of trust and reputation due to the uncertainty of how such information was obtained (may be hidden or distorted by witnesses in their own interests) [110].

Sociological information. The basis of this knowledge is the social relations between agents (trade, competition, cooperation, etc.) and what roles they play in society. Both social relationships and user roles influence his behavior and interaction with other agents. Social network analysis (SNA) methods are used to analyze social structures and their relational aspects [111]. Only a few models use this type of information to improve the calculation of trust and reputation values, as modern systems contain virtually no such information. However, in the future, increasing the complexity of multi-agent systems, enriching them with various complex relationships will increase the importance of this type of information.

Contextual dependence. Obviously, trust/reputation is generally context-dependent, i.e. situation-dependent. Most often, computational models consider the context of the subject area: if we trust the teacher of the Ukrainian language in matters of spelling, it does not mean that we should trust him in matters of organizational management. In multi-context trust/reputation models, reputation/trust values are associated with each user for each context. Usually, information in systems is not enough, so a good multi-context system must use it properly in different contexts. The introduction of multiple contexts complicates the system and at this stage of development, modern systems use only one context in connection with the solution of limited, specific tasks (all user actions occur in one context).

Assumptions about user behavior. Ability to deal with agent manipulation. There are three types of models:

1. The model clearly does not take into account such users, it is believed that a large number of users who provide reliable information neutralizes unreliable.

2. The model assumes that agents can hide information or overestimate/underestimate, but they never lie.

3. The model uses special mechanisms to combat liars.

«Discrimination». To calculate the trust/reputation of the model, sometimes mechanisms are used that distinguish users who enjoy a certain reputation into groups on certain grounds (for example, behavior).

Using global or local values. The value of reputation is global [120] (one for each user), the value of trust is personal (for each pair of users). In the first case, the value of reputation is calculated based on the opinions of users who have interacted with data in the past. This value is available to all users and is updated each time a new thought appears. In the second case, the personal value of user *X* is set from the point of view of user *Y* based on direct experience, indirect information obtained from other users, known relationships between users, etc.

Global values are used today in most online systems designed for scenarios with thousands or even millions of users. The size of these scenarios makes it virtually impossible to re-interact between the same users, and therefore reduces the incentives for users to collaborate to build profitable relationships. The reliability of these systems depends on the number of opinions. A large number of opinions minimizes the risk. In simple questions, the use of global values is permissible, but not for complex and subjective issues [107, 109].

Personal/local values are used in small and medium-sized systems, where interactions are frequent and strong connections are established between users. This reasoning is even more important in the context of social networks.

Reputation systems [108]. Reputation systems must have three properties:

1. Agents must be long-lived so that future interactions are expected in each interaction. Therefore, it must be difficult for an agent to change his «nickname» to get rid of the interaction history.

2. Estimates of current interactions should be published and disseminated. This is provided by the protocol in the system, and for distributed systems as opposed to centralized systems this is a problem. For the system to work, participants must be prepared to provide assessments, and appropriate incentive mechanisms must be developed.

3. Estimates of past interactions should be considered when making decisions about current interactions. It depends on the ease of use of such a system. Note also the main differences between the systems of reputation and trust:

1) trust systems calculate values that reflect the participant's subjective opinion about the reliability of the user, and reputation systems display the value of the user's reputation based on information from the whole community;

2) transitivity is a direct component in systems of trust, and reputation systems, as a rule, only indirectly take into account transitivity;

3) trust systems, as a rule, receive the input of subjective and general measures (reliability) of trust, while reputation systems – information or assessments of specific (objective) events, such as transactions.

Reputation network architecture. Architecture determines how reputation ratings and values are transmitted between members of the reputation system.

Centralized reputation systems. This system collects assessments of the actions of the participant, which were provided by other members of the community with direct experience. There is a center that collects and publishes them, calculates the value of reputation. In the future, participants can use this information to decide whether to interact or not. We are dealing here with the following aspects:

1. Centralized communication protocols, which provide an opportunity both to provide participants with assessments of the transaction partners of the center, and to obtain from the center the value of the reputation of a potential transaction partner.

2. The reputation calculation model used by the center to derive the reputation values of each participant based on the estimates obtained and possibly other information.

Distributed reputation systems. In a distributed system, there is no center for collecting ratings and obtaining reputation values. Distributed assessment repositories are used instead, or even each participant can keep their thoughts on the experience with other participants and send this information upon request. The user finds these repositories or receives ratings from community members who have direct experience with a potential partner to decide whether to participate in the transaction. Then the user calculates the value of the reputation of a potential partner, based on the received assessments and their direct experience.

Note the following aspects:

1. Distributed communication protocol that allows participants to receive ratings from other members of the community.

2. The method of calculating the reputation used by each agent on the basis of estimates and possibly other information.

Joint filtration systems. Shared filtering systems (such as Last.Fm) are similar to reputation systems in that they collect community member ratings. However, they also have fundamental differences. The assumption of such systems is that different people have different tastes and evaluate things differently. If two users evaluate many things in the same way, then they have similar tastes and are called neighbors. This information can be used to recommend things that one participant likes, his neighbors. Implementations of this method are often called «recommended systems». They should not be confused with reputation systems, which are based on the opposite assumption that all members of the community must agree on the effectiveness of user interactions, or on the quality of goods or services. Co-filtration systems take into account individual taste ratings, while reputation systems do not. Joint filtering systems rely on the reliability and honesty of participants, reputation systems a priori rely on their unreliability.

Computational models (metrics). Simple summation or average of estimates. The value of reputation is the sum of positive and negative feedback. An example is eBay. This method of calculation is primitive and the value of reputation is rough, and yet they are quite important. It has the advantages of this method as transparency and user-friendliness. More sophisticated schemes are used in Epinions and Amazon, which weighs estimates based on reputation, assessment time, distance, etc.

Marsh asked questions about understanding trust, as well as questions about using trust in literature and in everyday life. In his work, Marsh [9] models only direct trust. He proposes a set of variables and their method of combining to obtain a single value of confidence in the range [–1; 1] (although according to him there is no complete trust or distrust). Each of the trust variables depends on the context and time. Marsh identified three types of trust:

– basic, in all contexts;

– common, between two people in all contexts;

– situational, between two people in specific conditions.

These trust values are used to calculate the risk (which also depends on the costs and benefits) associated with the situation and the intended competence of the target user, in order to help the agent, decide to interact with another agent based on some value. Cooperation is possible if situational trust is above the threshold. Also, decision-making is extended by the concept of «reciprocity»: «you to me, me to you» (to modify the value of trust, ie if user *X* has helped *y* in the past, and there is no answer, the value of trust will be reduced).

Advogato Trust Metric (flow model). The Advogato Trust Metric algorithm formed the basis of the blog http://www.advogato.org and allowed to protect the community from such negative social phenomena as, for example, spam, trolling. This algorithm allows to identify community members who enjoy its trust. A community trusts member if they are trusted by the core. The «core» of the community (or «core of trust») is formed of several members with the highest trust. Relationships of trust in society are modeled by a graph, the vertices of which are members of the community, and the edges are built on the basis of certification by each member of the community of those members whom he trusts. In the simplest case, kernel trust in other members could be determined by having a path on the trust graph from the vertices of the kernel to the vertex of each participant (trust transitivity is used), but the Advogato Trust Metric algorithm uses a more sophisticated approach based on «trust flow» through the count. The main idea of the algorithm is to find the maximum flow through the graph, after which all those participants whose vertices receive a non-zero flow of confidence at the input will have confidence.

A person begins to trust the network more and more private information, until he receives one or another negative experience. The fact that excessive openness and openness in social networks is dangerous has been repeatedly confirmed. Here is just one figure: 88 % of private photos of an open nature, posted on social media, are stolen and promoted on porn sites without notifying the owners.

So far, we have talked about the fact that a person's psychological properties have an impact on his behavior on social networks. It is logical to assume that on the basis of this material can be solved and the inverse problem. According to Shuotian Bai of the University of the Chinese Academy of Sciences in Beijing, in 2012 a group of researchers developed an online test to determine a person's psychological portrait by the pattern of his behavior on social networks such as Facebook or Renren (China's popular social network).

We like to talk about ourselves and this is not news [111]. In everyday life, people devote about 30–40 % of all conversations to this. But on social media, that number is rising to a gigantic 80 percent! Why so? The face-to-face conversation takes place spontaneously and emotionally – there is no time to think about what to say – you need to have time to read the facial expressions and body language of the interlocutor. During the online conversation we have the opportunity to build and improve it. This is what psychologists call self-presentation: positioning ourselves as we want to be seen by others.

In the process of self-presentation there are such strong feelings that even viewing your own profile on Facebook can increase our self-esteem.

Self-presentation and strengthening of relations. Self-perception: 68 % of people say that they share information about themselves in order to make it clear who they are and what worries them. The other 78 % of people – because it helps to stay in touch with people. Experiments have shown that the perception of an idea as potentially contagious at the brain level is related to thoughts about other people.

Facebook, with more than 2 billion active users per month, is a great example of a platform where people like to «like». Since Facebook introduced the «Like» button, it has been clicked by more than 1.13 trillion times and this number is growing every day.

The ability to manipulate an opinion depends on the reputation vector, and the greater the reputation, the greater the ability to manipulate the opinion of another user in the given. These manipulations do not depend on positive or negative opinions.

Reputation in the modern world is becoming a popular indicator of the activities of individual politicians, organizations, authorities, cities, territories and states. The relevance of the phenomenon is explained by the transition to the «economy of intangible assets and corporate reputation» [27, 28]. Since reputation can be possessed only by the subject of social action (individual, organization, social movement, state, etc.), the value principles of its activity, methods and goals are actualized. The availability of information makes reputation an important factor influencing the activities of an entity. In today's world, thanks to the development of communication technologies, professional information becomes available to a wide range of people, information literacy and experience in processing message sources are formed.

Reputation became a separate subject of scientific research only in the second half of the twentieth century, but its manifestations attracted attention in the early stages of formation of political thought. An important component of the study of the phenomenon of reputation is marketing research, which has formulated such categories as «negative bias», describing the mechanism of influence of negative information on the impression of the subject, and «trust asymmetry», which determines the stronger impact of negative information on reputation compared to positive. In general, reputation is what other people think of us. As C. Fombran noted, reputation is the basic idea within which an individual exists in society. The researcher paid great attention to the information flows that create the subject of reputation, their role in the management of this phenomenon. He notes that reputation is a reflection of the actions taken by the entity in the past. This allows you to assess its subsequent behavior, to identify possible types of stakeholder interaction. Thus, reputation establishes a connection between the past and future behavior of the subject, its probable characteristics.

Researchers identify types of reputations in the context of personality leading features:

– mythological reputation, artificially created for electoral or other political purposes;

– real reputation, which is formed in the process of policy and is an objective reflection of its positive and negative qualities (this is especially important in a competitive environment, as it complicates the destruction of reputation by finding inconsistencies in its composition);

– one-dimensional reputation is created provided that the politician and his electorate have common unambiguous positions, goals and ideals;

– multidimensional reputation is more complex in construction, as it is based on the views of different groups and program ambiguity of the policy [25].

Analyzing the presented definitions, we can conclude about two stages of conceptualization of the concept of «reputation». In the first stage, this concept is considered as the impression or perception of the subject of reputation by different target audiences. Behavior is not influenced by abstract ideas or perceptions, but by evaluations. Therefore, in the second stage of conceptualization, the concept of «reputation» is most often revealed through the assessment of the activities and behavior of the subject.

Thus, during the evolution of the meaning of the concept of «reputation» has acquired two main dimensions:

1. The level of positive assessment of the subject in relation to certain criteria.

2. The level of information that reflects the level of collective recognition in their field.

Therefore, the quantitative parameter of reputation, which increases the security of information in social networks, we determine the complex indicator of the two main dimensions of «reputation». Each of the measurements is a dimensionless quantity that is in the range from 0 to 1.

Therefore, we are a quantitative parameter of reputation, which increases the security of information on social networks. We determine by a complex indicator of the two main dimensions of «reputation», each of which is a dimensionless quantity. It is in the range from 0 to 1.

According to the definition of the value of reputation, the value of the confidence factor is calculated, also in relative units. The value of trust can take values from 0 to 1. More detailed values of the reputation parameter and the basis of this determination of the confidence factor is obtained by regression analysis.

3.2 MODEL FOR DETERMINING THE SECURITY OF INFORMATION UNDER THE TRUST BETWEEN USERS AND THE AMOUNT OF INFORMATION IN THE NETWORK

In the classical approach to the problem of personal data protection, there are many threats of loss of trust between users, which can be represented as a function:

$$T_i = F\left(\left[D_j, D_n, D_m, D_k\right]\right), \tag{3.1}$$

where T_i – set of threats of loss of trust between users; D_j – trust in the provision of services (a person trusts the party in the provision of quality services or resources by the provider); D_n – delegation trust describes the trust in the user (representative) acting and making decisions on behalf of the party he trusts; D_m – access trust describes the trust on the part of the (provider) to the user who is granted access to resources. This is access control. Used in authentication systems; D_k – contextual trust determines the extent to which a participant believes in the necessary systems and institutional mechanisms that support transactions and ensure network security.

The loss of such a quality as trust is a process that has a time interval. Denote the amount of information in the system – *I*. The flow of information outside the information system through *dI*, the rate of change of this flow – dI/dt.

It is logical that if the flow and the rate of change of flow are zero, then there is no leakage of information:

$$dI = 0;\ \frac{dI}{dt} = 0. \tag{3.2}$$

Leakage of information depends on the security of the system and the measures taken to neutralize threats to the security of personal data.

Let *Z* be an indicator of information system security. Let's make an equation:

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + \left(C_v + C_k\right) I - L_2\left(I_0^2 \sin^2 \omega t\right) - L_3\left(I_0^3 \sin^3 \omega t\right) - \ldots; \\ \dfrac{dZ}{dt} = D_i - I\left(C_{d1} + C_{d2}\right) - K_2\left(Z_0^2 \sin^2 \omega t\right) - K_3\left(Z_0^3 \sin^3 \omega t\right) - \ldots . \end{cases} \tag{3.3}$$

To solve the system of equations (3.2) we write the system (3.3) in the form:

$$\begin{cases} \dfrac{dI}{dt} = \alpha Z + \beta_1 I - \sum\limits_{k=2}^{\infty} L_k I_0^k \sin^k \omega t; \\ \dfrac{dZ}{dt} = \beta_2 I + \gamma - \sum\limits_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t, \end{cases} \tag{3.4}$$

where $\alpha = Z_p,\ \beta_1 = C_v + C_K,\ \beta_2 = -\left(C_{d2} + C_{d1}\right),\ \gamma = D_i$.

Next, we use the exclusion method:

$$\frac{dZ}{dt}=\beta_2 I+\gamma-\sum_{k=2}^{\infty}K_k Z_0^k\sin^k\omega t\Rightarrow I=\frac{1}{\beta_2}\left(\frac{dZ}{dt}-\gamma+\sum_{k=2}^{\infty}K_k Z_0^k\sin^k\omega t\right)\Rightarrow$$
$$\Rightarrow\frac{dI}{dt}=\frac{1}{\beta_2}\left(\frac{d^2Z}{dt^2}+\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_k Z_0^k\sin^{k-1}\omega t\cos\omega t\right)\right). \quad (3.5)$$

Substitute into the first equation of the system:

$$\frac{1}{\beta_2}\left(\frac{d^2Z}{dt^2}+\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_k Z_0^k\sin^{k-1}\omega t\cos\omega t\right)\right)=$$
$$=\alpha Z+\frac{\beta_1}{\beta_2}\left(\frac{dZ}{dt}-\gamma+\sum_{k=2}^{\infty}K_k Z_0^k\sin^k\omega t\right)-\sum_{k=2}^{\infty}L_k I_0^k\sin^k\omega t \quad (3.6)$$

or

$$\frac{d^2Z}{dt^2}-\beta_1\frac{dZ}{dt}-\alpha\beta_2 Z=-\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_k Z_0^k\sin^{k-1}\omega t\cos\omega t\right)-\beta_1\gamma+$$
$$+\beta_1\sum_{k=2}^{\infty}K_k Z_0^k\sin^k\omega t-\beta_2\sum_{k=2}^{\infty}L_k I_0^k\sin^k\omega t. \quad (3.7)$$

Find the solution of the corresponding equation:

$$Z''-\beta_1 Z'-\alpha\beta_2 Z=0. \quad (3.8)$$

The characteristic equation has the form: $\lambda^2-\beta_1\lambda-\alpha\beta_2=0$.

We will consider only the case for the positive discriminant of this equation:

$$D=\beta_1^2+4\alpha\beta_2>0\Rightarrow\lambda_{1,2}=\frac{\beta_1\pm\sqrt{\beta_1^2+4\alpha\beta_2}}{2}.$$

And

$$Z_{gse}(t)=c_1 e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}+c_2 e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}$$

– general solution of the equation (3.8).

To find the general solution of the inhomogeneous equation, we use the method of variation of arbitrary constants:

$$Z_{gse}(t)=c_1(t)e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}+c_2(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}, \quad (3.9)$$

where $c_1'(t), c_2'(t)$ will be found from the system of equations:

$$\begin{cases} c_1'(t)e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}+c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}=0; \\ c_1'(t)\dfrac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}+ \\ +c_2'(t)\dfrac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}=N(t), \end{cases} \quad (3.10)$$

where

$$N(t)=-\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)-\beta_1\gamma+$$
$$+\beta_1\sum_{k=2}^{\infty}K_kZ_0^k\sin^k\omega t-\beta_2\sum_{k=2}^{\infty}L_kI_0^k\sin^k\omega t. \quad (3.11)$$

We will get:

$$c_1'(t)e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}=-c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\Rightarrow$$

$$\Rightarrow c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\left(-\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}+\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}\right)=N(t), \quad (3.12)$$

or

$$c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\sqrt{\beta_1^2+4\alpha\beta_2}=-N(t). \quad (3.13)$$

Then we will get:

$$c_2(t)=-\frac{1}{\sqrt{\beta_1^2+4\alpha\beta_2}}\int N(t)e^{\frac{-\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\mathrm{d}t, \quad (3.14)$$

and

$$c_1(t)=\frac{1}{\sqrt{\beta_1^2+4\alpha\beta_2}}\int N(t)e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\mathrm{d}t. \quad (3.15)$$

Mathematical model in the final form will look like:

$$Z(t)=\frac{e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}}\int N(t)e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\mathrm{d}t-\frac{e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}}\int N(t)e^{\frac{-\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\mathrm{d}t. \quad (3.16)$$

As a result, we obtained the results in general: the dependence of personal data protection on trust is proportional to the constant parameters of protection.

In order to confirm the obtained results, we will perform modeling in the MatLab environment.

In **Fig. 3.1** the dependence of personal data protection (in relative units) on the amount of information in the system – the main parameter, and the parameter of trust in information.

In **Fig. 3.2** the dependence of personal data protection (in relative units) on the parameter of trust in information – the main parameter, and the amount of information in the system is given.

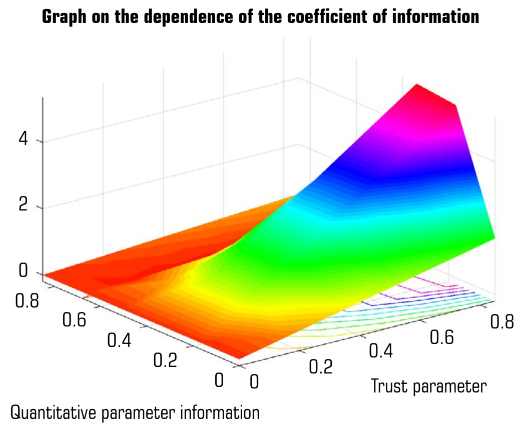


Fig. 3.1 Dependence of personal data protection on the growth of information in the system

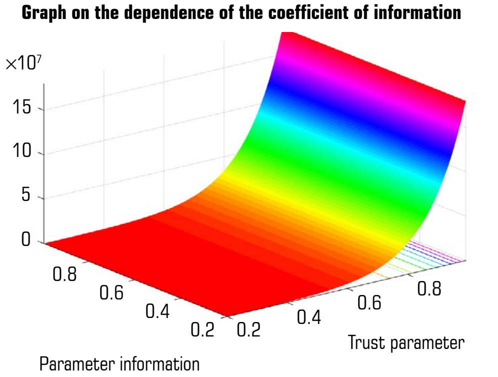


Fig. 3.2 Dependence of personal data protection on trust between users

As we can see from the simulation results, the protection of personal data directly depends on the amount of information and the parameters of trust in this information. The protection of personal data increases with the amount of reliable information and the amount of general information. This fully confirms the accuracy of the proposed method of assessing the protection of personal data.

This section is devoted to the method of assessing the dependence of personal data protection on the amount of information in the system and trust in social networks. Simulations for different types of changes in trust parameters and the amount of information in the system are performed. All variants of solving the equation near the steady state of the system proved that, based on the conditions of the ratio of dissipation and natural frequency of confidence, and the attenuation of the latter to a certain value is carried out periodically, with decaying amplitude, or exponentially decaying law. The obtained graphic materials fully showed that the protection of personal data increases with the growth of factors of trust in information. Dependence of protection of personal data on trust is proportional at constant other parameters of protection. With the growth of the amount of information in the system and trust in information, the total indicator of information protection, when modeling by the proposed method, increases at a rate of 9 % more than by modeling by other methods, which is quite a suitable result.

3.3 MODEL OF INFORMATION DEFENSE IN CORRESPONDENCE WITH THE PATH OF INFORMATION TRANSFER

Analysis of the interaction of external influences and defenses can be presented in the form of a theoretical-group model [113–115]. This is a mathematical model of collective behavior.

Several participants influence the situation, and their interests and the path to the goal are different. With this representation of the interaction of dynamic systems, we have the equation:

$$S_i,\ i=[1,n]. \tag{3.17}$$

There are three possible behavioral strategies. In general, these strategies can be classified as follows:

1) antagonistic strategy, when participants have opposing interests;

2) cooperative strategy, when everyone has a common goal and their strategies are agreed;

3) strategy of indifference, when the strategy of the *j*-th player does not depend on the strategy of the *i*-th player. That is, its length of path to information does not affect the protection of information.

There are other types of strategies – pure or mixed [113]. In pure strategies, a deterministic approach is assumed, and as follows from theory, rarely leads to equilibrium decisions. In contrast, in mixed strategies with a stochastic approach, the range of equilibrium solutions expands significantly.

To improve the model, we assume that we do not consider the third type of this classification. But consider a mixed strategy.

The processes of external influences and defenses are an antagonistic strategy, or in general – mixed. With small deviations in the information with a priori data of reputational behavior of the social network, it is possible to imagine a model of interactions and phase states of external influences and protections. It should be noted that in the known works there is no idea of a telecommunication network in the form of a theoretical-group model with an antagonistic strategy of behavior.

For further improvement, we assume that the main parameters of external influences are known and accept them as deterministic. This fact is due to the influence of many uncertain, random conditions.

As a result of accidental threats from external influences: y_i, $i=[1,n]$, where: n – number of external influences.

The network has corresponding dynamic interactions that can be detected and analyzed as a result of measurements and observations, and are characterized by a vector $\vec{y}(t)$. Then the dynamics of random changes in the state of the parameters of external influences can be described by a system of differential equations:

$$\frac{\vec{x}(t)}{dt}=S(t)\vec{x}(t)+U(t)\vec{x}(t)+W(t)\vec{q}, \tag{3.18}$$

where $x(t)$ – vector of state of external influences parameters; $S(t)$ and $U(t)$ – state and control matrix, respectively; $u(t)$ – the control vector of the corresponding parameters of the information security system; $q(t)$ – a random process that is approximated by white Gaussian noise; $W(t)$ – a matrix that scales random perturbations.

The observed parameters of the state of external influences are described by a system of algebraic equations:

$$\vec{y}(t)=N\left(\vec{x}(t),t\right), \tag{3.19}$$

where $N(t)$ – observation matrix.

It can be assumed that if the whole range of external influences, we observe and take measures to prevent them, i.e., protection is carried out with one or another probability.

In the general case, the system of equations can be nonlinear. Then, without specifying the nonlinearity itself, the vector equation can be represented as:

$$\frac{\vec{x}(t)}{dt}=F(t)\left(\vec{x}(t),\vec{y}(t)\right), \tag{3.20}$$

where $F(t)$ – the state matrix of dimension $n\times n$, in this case $F(t)=diag\left(f_i,\, i=[1,n]\right)$.

The success of the problem of protection in relation to external influences depends on available resources: $r_k=r_k\left(\vec{x}(t),t\right)$, $k=[1,K]$, as well as on known a priori probabilities: $p_i=p_i\left(\vec{x}(t),t\right)$, $i=[1,n]$. But we need to take into account the dynamics of changes in the state of the system over time, then the improved equation will take the form:

$$\frac{\vec{x}(t)}{dt}=D(t)\left(\vec{x}(t),\vec{y}(t),t\right). \tag{3.21}$$

Available resources r_k in the information protection system are determined by physical quantities. Therefore, the entire resource can be represented as the total amount:

$$r_k\left(\vec{x}(t),t\right)=\sum_{i=1}^{n}c_{ik}y_i,\ y_i\geq 0,\ k=[1,K],\ i=[1,n], \tag{3.22}$$

where c_{ik} – there is a connection between the i-th influence and the k-th protection.

The presence of a connection is determined by the matrix C, which consists of zeros and ones, zero has no connection, one – connection exists.

The dynamics of the process state is determined by the solution of equation (3.22), respectively, for $\vec{y}(t)$, which depends on the parameters c_{ik}, p_i, r_k. Moreover, it should be noted that the resource parameter includes a coefficient that takes into account the length of the information path in the social network.

Thus, the model of the state of the dynamics of influences takes the following form:

$$\frac{\vec{x}(t)}{dt}=F(t)\left(\vec{x}(t),\vec{y}(t),t\right), \tag{3.23}$$

$$\vec{y}\left(\vec{x}(t),t\right)=\operatorname{argmax}\left[H(Y)\sum_{i=1}^{n}c_{ik}y_i=r_k\left(\vec{x}(t),t\right)\right]. \tag{3.24}$$

In the considered unbalanced system there are two main processes:

1. The flow of external influences.
2. Threats of external influences.

Denote the flow of external influences through $V\left(\vec{x}(t),\vec{y}(t),t\right)$, and external influences through $Z\left(\vec{x}(t),\vec{y}(t),t\right)$. These variables depend on the state of the vectors $\vec{x}(t)$ and $\vec{y}(t)$.

Under the assumption that the time of threat of external influence is longer than the time of appearance of the influence itself, it is possible to write the following, in the general case, a nonlinear system of equations:

$$\frac{\vec{x}(t)}{dt}=V(t)\left(\vec{x}(t),\vec{y}(t),t\right), \tag{3.25}$$

$$\varepsilon\times\frac{\vec{x}(t)}{dt}=Z(t)\left(\vec{x}(t),\vec{y}(t),t\right). \tag{3.26}$$

where ε – diagonal matrix, which determines the effectiveness of external influences in the network.

The formation of a model of the form (3.26) for a process with constraints and different types of resources remains an unsolved problem. Such a model can be built only for those cases when the dynamics of the process is Markov, for the limitations of the balance type.

In this case, we can assume that the dynamics of the process isof the Markov type, because it does not matter when and how the network went into its current state, but only what state the network is in at the present time. Therefore, we will consider the general case of the presence of external influences in the network. The protection vector will be a function of the number of external influences: $\vec{z} = f\left(y_1(t), y_2(t) \ldots y_n(t)\right)$, then in the absence of external influences we have $\vec{z} = f(0)$, in the presence of a flow of external influences $\vec{z} = f(\infty)$.

The rate of change of the *i*-th influence is determined by the appearance of new influences $k_i \times y_i$. Let's take another assumption: k_i – the weight of the impact is assumed to be constant, i.e., k_i=const, in the second it is assumed that the old influences $g_i y_i$, disappear with high-quality system protection. Coefficient g_i, directly depends on the amount of resource spent r_i, spent on one external influence:

$$g_i = g_{i0} - \mu_i r_i,\ g_{i0}, \mu_i \geq 0, \tag{3.27}$$

where μ_i – weighting coefficient of controlled influence on the *i*-th external influence.

Then we get the equation:

$$\frac{dy_i}{dt} = \varepsilon_i y_i(t) + \mu_i w_i(t),\ i = [1, n], \tag{3.28}$$

where $w_i = r_i y_i$ – this is the amount of resource spent on the *i*-th impact.

We will consider the stationary process with fixed at time *t* interaction of protection and external influences on the information protection system in the social network. For this process we define an a priori characteristic. For each *i*-th impact, we know the number of regulatory resources required to neutralize external influences – a_i, then the parameter v_i, will look like:

$$v_i = \frac{a_i y_i}{\sum\limits_{i=1}^{n} a_i y_i};\ 0 \leq v_i \leq 1;\ \sum_{i=1}^{n} v_i = 1. \tag{3.29}$$

The steady state of this process will be determined by the model of the species:

$$(\omega) = \sum_{i=1}^{n}\left(\omega_i \ln\frac{v_i}{\omega_i} + \omega_i\right) \to \max. \tag{3.30}$$

Taking into account expression (3.28) we obtain:

$$\omega = a_i y_i \frac{\sum\limits_{i=1}^{n} \omega_i}{\sum\limits_{i=1}^{n} a_i y_i}. \tag{3.31}$$

Substituting (3.28) into (3.31), we obtain:

$$\frac{dy_i}{dt} = y_i\left(\varepsilon_i + a_i \varphi(y)\right). \tag{3.32}$$

where $\varphi(y) = \sum\limits_{i=1}^{n} \omega_i \Big/ \sum\limits_{i=1}^{n} a_i y_i$ is monotonically unprofitable.

The approximation coefficients are negative, i.e.:

$$\varphi(Y)=\sum_{s=1}^{n}v_s y_s(t). \tag{3.33}$$

Substituted the expression 3.28 at 3.30 we get a system of equations that characterize the dynamics of coexistence of external influences and protection of information in the social network:

$$\frac{dy_i(t)}{dt}=y_i(t)\left(\varepsilon_i-\sum_{s=1}^{n}v_s y_s(t)\right). \tag{3.34}$$

If we use a quadratic approximation, we obtain a nonlinear system of equations in the form:

$$\frac{dy_i(t)}{dt}=y_i(t)\left(\varepsilon_i-\sum_{s=1}^{n}v_s y_s(t)-\sum_{s=1}^{n}\sum_{j=1}^{n}v_s y_s(t)\vartheta_j y_j(t)\right). \tag{3.35}$$

Let's convert the obtained differential equation to a difference one. Let's mark t_k – discrete time. Then we will have:

$$\frac{dy_i(t_{k+1})-dy_i(t_k)}{t_{k+1}-t_k}=y_i(t)\left(\varepsilon_i-\sum_{s=1}^{n}v_s y_s(t)-\sum_{s=1}^{n}\sum_{j=1}^{n}v_s y_s(t)\vartheta_j y_j(t)\right), \tag{3.36}$$

where $t_{k+1}–t_k=T_D$ – discretization interval.

Then for discrete time we get:

$$y_i(k+1)=y_i(k)+T_D\left[y_i(k)\left(\varepsilon_i-\sum_{s=1}^{n}v_s y_s(t)-\sum_{s=1}^{n}\sum_{j=1}^{n}v_s y_s(k)\vartheta_j y_j(k)\right)\right], \tag{3.37}$$

or

$$y_i(k+1)=y_i(k)(1+T_D)\left[y_i(k)\left(\varepsilon_i-\sum_{s=1}^{n}v_s y_s(t)-\sum_{s=1}^{n}\sum_{j=1}^{n}v_s y_s(k)\vartheta_j y_j(k)\right)\right]. \tag{3.38}$$

This model allows to perform analysis for various specific parameters and interactions of attacks and defenses.

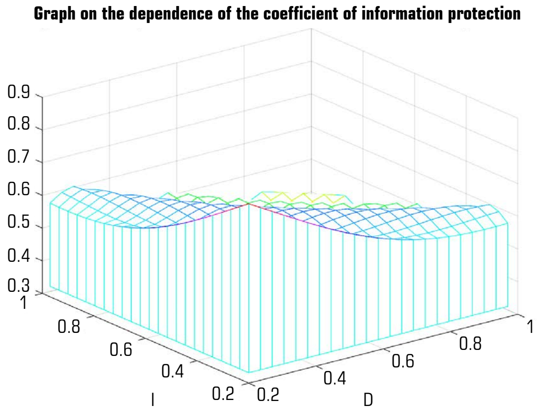
To use this model to determine the dependence of the protection factor of information (**Fig. 3.3**) on the average length of the path of information dissemination, we use equation 3.36 and assumptions.

The average path length in the Barabash – Alberta (BA) model increases on average as the logarithm of the network size. The exact form has a double logarithmic correction [114] and looks like: $l\sim \ln N/\ln\ln N$, where N – the number of paths between vertices in the network.

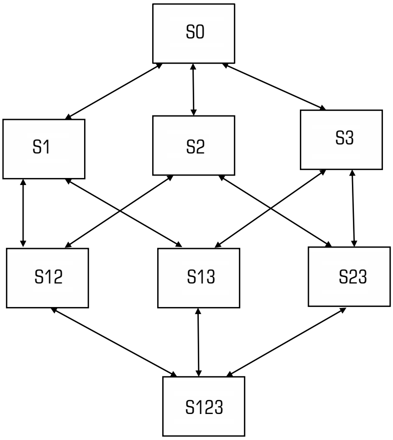
We introduce a coefficient that takes into account the average length of the information path in the social network: $\gamma=\left(\frac{\ln\ln n-n}{n(\ln\ln n)^2}\right)$, where n – the number of vertices in the network.

The BA model has a systematically shorter mean path than a random graph.

Using the improved model, we will model the process of information protection in the social network taking into account the coefficient of the path length of information in the social network. The simulation results are presented in **Fig. 3.4**.



⬡ **Fig. 3.3** Dependence of the average path length in the BA model for power networks on the number of nodes, where *I* is the average path length, *D* is the number of nodes in the network



⬡ **Fig. 3.4** Graph of the system of states of a random process

From the above graph we see that with increasing confidence and the length of the information path, the protection of information does not increase. This is because the increase in the protection factor is inhibited by the increase in the length of the information path. That is, increasing the length of the information path leads to a decrease in the coefficient of information protection. In this case, the confidence factor cannot compensate for the negative impact of the coefficient of the path of information. At the maximum information path length factor, the confidence factor cannot compensate for the decrease in the information protection factor and the system becomes vulnerable. This is fully confirmed by theoretical calculations, which proves the adequacy of the improved model.

Thus, the model of information protection of the social network is improved, where the antagonistic strategy is implemented. Based on the creation of a database of information vulnerabilities in social networks, it is possible to set the task of predicting the most effective threats to information security of a particular object of influence, taking into account in addition to general parameters, the parameter of information path length in the general network. The adequacy of the model makes it possible to consider the matrix of ways of disseminating information as a field of states of the object in the process of changing its states. As a result of improving the model, it is possible to analyze unbalanced states in the grouping of the network, which allows to prove the possibility of equilibrium states and determine the limit of stability of dynamic interdependent networks at different values of efficiency and different sampling intervals. The analysis showed that at high efficiency of influences the smaller interval of sampling is necessary for maintenance of system in a steady state.

3.4 METHOD OF CALCULATING THE SECURITY OF INFORMATION FOR THE NETWORK ELEMENTS CLUSTERING

Clustering is a local characteristic of the network [111]. It characterizes the degree of interaction between the nearest neighbors of the node. In most networks, if node *A* is connected to node *B* and node *B* is connected to node *C*, there is a high probability that node *A* is connected to node *C* (our friends' friends are usually also our friends) [117]. The clustering coefficient of a given node is the probability that the two nearest neighbors of this node are themselves the nearest neighbors [121].

The clustering factor corresponds to the ratio of the actual number of connections between its neighbors and their potential number. The clustering factor can be averaged for any part of the network or for the network as a whole, becoming its integral characteristic.

The clustering factor is a metric that is more efficient than density and is increasingly used in the social sciences [114]. The clustering factor is the degree that determines how much nodes tend to cluster [106]. For example, in a network of friends, it is likely that two of my friends are friends with each other. That is, it is some estimate of network fragmentation. With high clustering, it can be expected that the virus will spread only in a certain subgroup (cluster) [116]. With low clustering, there is a high probability of rapid spread of the virus throughout the network.

Consider a mathematical description of the Markov process with discrete states and continuous time for the security threat information system, which are created by threats of two external influences, the first – using threats of the first and second vulnerabilities, the second – the first and third vulnerabilities (consider dependent threats). First of all, consider a system with failures and restores the characteristics of information security, the graph of the system of random process states for which is presented in **Fig. 3.4** (S_0 –initial state of the system, S_i – one of the vulnerabilities is detected and not eliminated in the system, S_{ij} – two vulnerabilities are detected and not eliminated in the system, S_{ijl} – all three vulnerabilities are detected and not eliminated in the system).

We assume that all transitions of the system from one state to another occur under the influence of the simplest streams of events with the corresponding detection intensity λ_i or elimination μ_i vulnerabilities, and the probability of instantaneous detection, as well as the elimination of several vulnerabilities, is too small. The transitions of the system to states S_{12} and S_{13} are associated with the appearance of real threats of the corresponding influences. The transition from state S_{23} to S_{123} characterizes the simultaneous occurrence in the system of both threats (in the detection of the first vulnerability in the presence of the second and third), which, as we see, is taken into account in this method of modeling.

This graph illustrates the correctness of the simulation with the dependence of threat threats on vulnerabilities. With a similar approach to the source and reduced security threat digits of the information system, we obtain the same graph of the system of states of a random process, because the data of the digraphs contain the same set of vertices and transitions between vertices.

Using this model, we can construct a system of Kolmogorov differential equations for the probabilities of states, solving which, we can calculate the probability of readiness of the information system for safe operation (stationary coefficient of readiness of the system for safe operation). Note that the construction of the considered Markov model (**Fig. 3.5**) does not require the use of any expert assessments – the input parameters of the model are stochastic parameters of threat vulnerabilities, which can be obtained from statistics on their occurrence (detection) and elimination.

Now we will build the desired Markov model of the system, which must take into account that the real threat of impact with any probability will be realized and will lead to a fatal failure of safety characteristics. The mathematical model of the violator allows to determine the value of the coefficient of readiness (or probability) for a certain impact on a particular information system Kran. The basis of this mathematical model is the interpretation of the complexity of the implementation of external influences by the violator San the probable amount of information about the potential threat of an attack that the infringer must possess in order to carry it out:

$$S_{an} = I\left(P_{0an}\right) = -\log_2\left(1 - P_{0an}\right). \tag{3.39}$$

Consider the external influence as a sequence of use by the violator of the vulnerabilities detected and not eliminated in the system, having the characteristics P_{0yr} and Syr, $r=1,\ldots,R$, entering a quantitative characteristic of complexity Sa ($Sa=I(P_{0a})$). Value Sa depends on the amount of information required by the violator for a successful external influence, the threat of which is created by R detected in the system and unresolved vulnerabilities:

$$S_a = I\left(P_{oa}\right) = -\log_2\left(1 - P_{oa}\right) = -\log_2 \prod\nolimits_{r=1}^{R}\left(1 - P_{oya}\right), \tag{3.40}$$

where

$$P_{oa} = 1 - \prod\nolimits_{r=1}^{R}\left(1 - P_{oyr}\right). \tag{3.41}$$

Using the appropriate logarithm property, you can write:

$$S_a = I\left(P_{oa}\right) = \sum_{r=1}^{R} I\left(P_{0yr}\right) = \sum_{r=1}^{R} S_{yr}. \tag{3.42}$$

If the values of the characteristics are known S_a and S_{ah} (the maximum complexity of the realized, including reflected, in a similar information system of influences), it is possible to determine the value of the coefficient of readiness of the violator to the external influence of complexity S_a:

$$K_{ra} = \begin{cases} \frac{S_{ah}}{S_a}, \text{ if } S_{ah} \le S_a; \\ 1, \text{ if } S_{ah} \ge S_a. \end{cases} \tag{3.43}$$

When designing a protection system, you can always find an information system that is used to process similar information, which records the implemented effects, which allows you to calculate the value S_{ah}.

Note that to solve this problem does not require the introduction of any expert assessments – the input parameters can be obtained from the relevant statistics, which are continuously maintained.

Having the ability to set the value of the coefficient K_{ra}, you can build the desired Markov model of information system protection. In **Fig. 3.5** shows a fragment of the graph of the state of random processes of the system with a fatal failure of the safety characteristics (**Fig. 3.4**), which illustrates the most important features of this model.

In **Fig. 3.5** includes the absorbing state S_p, which characterizes the failure that does not restore the security characteristics of the information system (critical external influence on the information system) – there are no ways out.

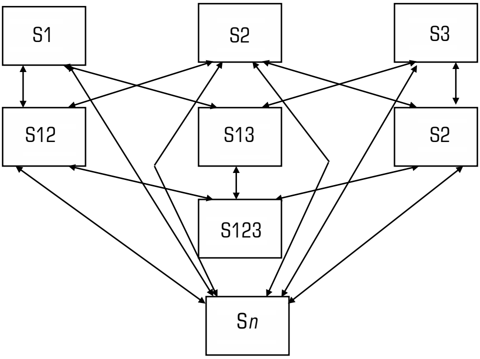


Fig. 3.5 A fragment of the graph of the state of random processes of the system with a fatal failure of the safety characteristics

Consider the transitions between the states S_1 and S_nS_{23} and S_n due to the presence in the system of threats of influences dependent on vulnerabilities.

The peculiarity of the transition from S_1 to S_n is due to the fact that the first vulnerability poses a threat to both attacks, therefore, the intensity of the transition from S_1 to S_n is defined as $K_{a2}\lambda_2 + K_{a3}\lambda_3$. The peculiarity of the transition from S_{23} to S_n is due to the fact that only one attack will be implemented by the violator. The state of S_{23} is characterized by the fact that the detected and unresolved second and third vulnerabilities, and as a consequence, the detection of the first vulnerability leads to the implementation of the first or second attack, so the intensity of the transition from S_{23} to S_n is defined as $K_{a1}\lambda_1 + K_{a2}\lambda_2$.

In order to determine the required security characteristics of the information system, a system of Kolmogorov differential equations is constructed for the graph constructed in this way, followed by a system of linear algebraic equations describing the stationary regime. By solving this system, you can get the probabilities of the desired states, including for the vertex, which absorbs, determining the probability of one of the potential attacks on the information system, respectively, the probability of readiness for its safe operation.

The value of the probability P_i of being in a certain state in the Markov model is interpreted as the average relative residence time of the system in the i-th state. To calculate the average absolute residence time of the system in each i-th state T_i in the system of Kolmogorov equations, you need to set zero to all derivatives $\left(P_i' \left(P_i' = 0\right)\right)$, exept P_0', if we assume that at the initial moment the probability of being in the state P_0 is equal to 1. Then, according to the theorem on image differentiation, in the Laplace transform the right part of the first equation will be equal to –1. In the right-hand sides of the equations, T_i is substituted for P_i, and a system of algebraic equations is solved for them. As a result, the average time of operation of the information system to failure (system with fatal failure) – to the implementation of its successful impact.

These two key security features of an information system can be used in designing a security system. In Markov reliability models, the failure rate parameter ω is determined (for a stationary site) as follows:

$$\omega = \sum_{i \in Q_+} P_i \sum_{i \in Q_-} \lambda_{ij}. \tag{3.44}$$

where Q_+ – set of states of system efficiency; Q_- – set of states of system failures; λ_{ij} – the intensity of the transition from the i-th operational state, the probability of finding a system in which, P_i in the j-th will cause an inoperable state.

To build an enlarged model of information system security threats, we again turn to **Fig. 3.5** and determine how the flow of security failures is formed. As you can see, the threat of impact occurs in three cases – in the transition from state S_{12}, in which the system is with probability P_{12} (in the Markov model, the probability of being in the state is interpreted as the relative part of the system in this state), to state S_{123} threats of influence), transitions are carried out with intensity λ_3 (taking into account the corresponding part of the time spent in the state S_{12} – with intensity $P_{12}\lambda_3$), during the transition from state S_{13}, in which the system is with probability P_{13}, to state S_{123}, the transitions are carried out with intensity λ_2 (taking into account the corresponding part of the time spent in the state S_{13} – with intensity $P_{13}\lambda_2$), in the transition from state S_{23}, in which the system is with probability P_{23} to S_{123}, the transitions are carried out with intensity λ_1 (taking into account the corresponding part of the time spent in the state S_{23} – with intensity $P_{23}\lambda_1$).

The failure flow defined in this way can be interpreted as the flow of the real threat of impact, which is created in the system with intensity λ_z:

$$\lambda_z = \omega = P_{12}\lambda_3 + P_{13}\lambda_2 + P_{23}\lambda_1. \tag{3.45}$$

Taking into account the obtained result, an enlarged Markov model of threat to the security of the information system as a whole, which is created by N threats of influences, can be built. The graph of the system of states of a random process which is presented in **Fig. 3.6**. The intensity of the transition to the absorbing state of S_n in this case is determined by the intensity of the real threats of influences λ_{zn} and the coefficients of readiness of the violator to a real attack, K_{rzn} $n=1,\dots, N$.

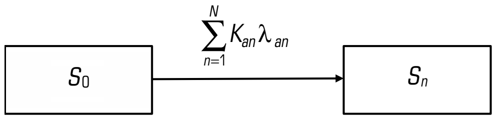


Fig. 3.6 An enlarged Markov model of information system security threat

Practical use of the enlarged model allows to simplify the task of modeling the protection system, reducing it to a number of simpler tasks. In this case, the initial set of threat threats that pose a threat to the security of the information system can be optimized (significantly reduced) using the method of dynamic programming, due to the strong dependence of threats on threat vulnerabilities (many threat threats are created by the same vulnerabilities).

In conclusion, we note that the most important results include substantiation of the correctness of the use of Markov processes in modeling key security characteristics of the information system, identified and investigated fundamental differences in the formulation and solution of the problem of modeling the reliability and security of information systems. systems. An important result of the study is the justification of the need to consider in the modeling of security characteristics as a security element should not be considered threats of impact, and – threats of vulnerability. As shown, this is due not only to the impossibility in the general case of a correct task (without any expert assessments) of the input parameters of the model, the ability to justify the requirements for input flows, but also the impossibility of building a correct model, because threats are generally dependent from threats of vulnerabilities.

Calculating or estimating the clustering factor can give an idea of the impact of the dissemination of unauthorized information by malicious users on the friendship with the nodes [109]. After the malicious node η is added to the contact list ν, η can access sensitive information ν and disclose it indiscriminately using social media tools such as bulletin boards, image posting, and more.

To develop a model for protecting information from the clustering factor, we make a notation:

$$\alpha = Z_p,\ \beta_1 = C_v + C_K,\ \beta_2 = -\left(C_{d2} + C_{d1}\right),\ \gamma = \left(\frac{\sum\limits_{v \in V} C_{v1}}{N^2}\right).$$

Where $\sum\limits_{v \in V} C_{v1}$ – the total number of connections in the network; N – the number of vertices in the network.

The dependence of the information protection indicator on the parameters of the information protection system in the social network is determined by the expression:

$$Z(t) = \int N(t) - e^{\frac{-\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}t} \frac{e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2 + 4\alpha\beta_2}} \mathrm{d}t - \int N(t) - e^{\frac{-\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}t} \frac{e^{\frac{\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2 + 4\alpha\beta_2}} \mathrm{d}t. \quad (3.46)$$

Solving this equation, taking into account the assumptions and limitations, we obtain the expression:

$$Z(t) = \int \left[\begin{array}{l} -\frac{1}{\omega} \sum\limits_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) - \beta_1 \times \left(\frac{\sum\limits_{v \in V} C_{v1}}{N^2} \right) - \\ - \beta_1 \sum\limits_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \times \sum\limits_{k=2}^{\infty} L_k I_0^k \sin^k \omega t \end{array} \right] \times$$

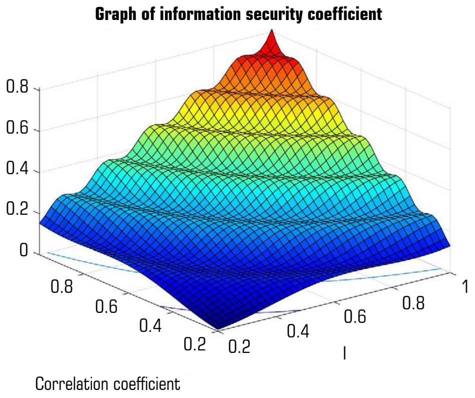
$$\times \left(\left(1 - e^{\frac{-\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}t} \frac{e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2 + 4\alpha\beta_2}} \right) - \left(1 - e^{\frac{-\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}t} \frac{e^{\frac{\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2 + 4\alpha\beta_2}} \right) \right) \mathrm{d}t, \quad (3.47)$$

where $\sum\limits_{v \in V} C_{v1}$ – the total number of connections in the network; N – the number of vertices in the network.

Expression 3.47 is an expression of a mathematical model of social network information protection, taking into account the clustering factor, which depends on the graph model of the entire social network system, namely the number of connections in the network and the number of vertices in the network. based on these data, the information is clustered. In order to verify the results, we will simulate the process of information protection depending on external influences. Assume that all coefficients are dimensionless, ie calculated in relative units. And the biggest impact is the unit, similarly to the clustering factor. In order to confirm the obtained results, we will perform modeling according to the developed model, taking into account external influences that are nonlinear.

The simulation results are shown in the graph of **Fig. 3.7**.

The analysis of the graph of **Fig. 3.7** shows that the influence of the clustering coefficient on the parameter of information protection in social networks is wavy in nature with a gradual increase in information protection. This is due to the clustering process itself. That is, clustering combines information on features that are more similar in the center, so the coefficient of clustering of information in the cluster is closest to the center and falls to the edge. But the greater the intensity of information, the more clusters and the greater the protection of information because it is much easier to protect information with the same characteristics than random information. This corresponds to the physical process and confirms the adequacy of the proposed model.



⬡ **Fig. 3.7** Graph of the dependence of information protection on the clustering factor

But the analysis of the proposed model would not be complete if we did not use the opportunity to assess the stability of the system according to the developed model. That is, having received a model with the parameters of information protection of the social network, we will assess the resilience of our system to external influences. To do this, we will determine the phase portrait of the information protection system of the social network using our equation:

$$\frac{d^2Z}{dt^2}-\beta_1\frac{dZ}{dt}-\alpha\beta_2 Z=-\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)-$$

$$-\beta_1\gamma+\beta_1\sum_{k=2}^{\infty}K_kZ_0^k\sin^k\omega t-\beta_2\sum_{k=2}^{\infty}L_kI_0^k\sin^k\omega t. \qquad (3.48)$$

The solution will be implemented in the program MatLab/Multisim.

As a result of modeling, we obtained a phase portrait of the protection system against clustering parameters at maximum values of external influences and clustering coefficient – 1, all other parameters of the protection system – 1. Additionally, we obtained a phase portrait of protection system at maximum influence and clustering coefficient – 0.5, all other parameters protection systems – 1. The obtained phase portraits are presented in the form of an ellipse, which indicates the stability of the information protection system.

Thus, in addition to the model of information protection depending on the clustering factor, developed a mathematical apparatus to increase the level of security of the information space of social networks, which is based on the analysis of the constructed phase portrait and transient analysis of information security. The technique allows to effectively investigate transients with the possibility of visualization of models (block diagrams) and research results.

3.5 IMPACT OF THE NOISE AND THE INTERFERENCE IN THE PROTECTION OF INFORMATION ON SOCIAL NETWORKS

In the real process of information protection in social networks, there are many factors that hinder the process of information protection. For example, an obstacle in the form of noise, which can completely hide the external influence on the protection system, so the mathematical model needs to be improved by calculating interference and interference. To do this, take the expression to determine *p* exponent in the absence of additive noise:

$$\sum_{m=0}^{p} a_m x\left(n-m\right)=0, \tag{3.49}$$

where $a_0=1$, then the characteristic polynomial will have the form:

$$A_z=\sum_{m=0}^{p} a_m z^{p-m}. \tag{3.50}$$

It has roots $z_k=e^{S_k}$, where $1\le k\le p$ and $S_k=1/T\left(\alpha_k+j2\pi f_k\right)$, S_k – characterizes the attenuation coefficient and the frequency of the *k*-th exponent. The following equations can be obtained in reverse time by inverting the linear prediction equation:

$$\sum_{m=0}^{p} b_m x\left(n-p+m\right)=0, \tag{3.51}$$

where $b_0=1$. Characteristic polynomial that has the form:

$$B_z=\sum_{m=0}^{p} b_m^* z^{p-m}. \tag{3.52}$$

Formed from complex-conjugate coefficients of linear prediction back, has roots:

$$z_k=\exp\left(-S_k^*\right)=\exp\left(\frac{1}{T}\left(-\alpha_k+j2\pi f_k\right)\right), \tag{3.53}$$

where $1\le k\le p$.

For the fading *q* exponent $\alpha_k < 0$ these roots of linear prediction forward A_z will fall into a circle of unit radius *z* – plane, and the roots of the characteristic polynomial B_z will, on the contrary, be outside this circle due to the attenuation coefficient $e^{-\alpha_k^T}$, corresponding to the growing exponent.

These properties of the location of the roots of polynomials A_z and B_z due to the properties of deterministic exponential functions.

Further improvement of the results is possible by using the method of decomposition by singular numbers. Linear forward and backward prediction errors can be recorded in the following form:

$$X_p^f a_p^f = -x_p^f + e_p^f,\ X_p^b a_p^b = -x_p^b + e_p^b, \tag{3.54}$$

where Toeplitz data matrices X_p^f, X_p^b and data vectors x_p^f, x_p^p are defined by expressions:

$$X_p^f = \begin{bmatrix} x(p)....x(1) \\ .... \\ x(N-1)... \end{bmatrix},\ x_p^f = \begin{bmatrix} x(p+1) \\ .... \\ x(N) \end{bmatrix},$$

$$X_p^b = \begin{bmatrix} x(p+1)........x(2) \\ .... \\ x(N)...x(N-p+1) \end{bmatrix},\ x_p^b = \begin{bmatrix} x(1) \\ .... \\ x(N-p) \end{bmatrix}. \tag{3.55}$$

A vector of linear prediction coefficients forward a_p^f, vector of linear prediction errors e_p^f, vector linear prediction back a_p^b and vector of back linear prediction errors e_p^b will be determined by expressions:

$$a_p^f = \begin{bmatrix} a^f(1) \\ .... \\ a^f(p) \end{bmatrix},\ e_p^f = \begin{bmatrix} e^f(p+1) \\ .... \\ e^f(N) \end{bmatrix},$$

$$a_p^b = \begin{bmatrix} a^b(p) \\ .... \\ a^b(p) \end{bmatrix},\ e_p^b = \begin{bmatrix} e^b(p+1) \\ .... \\ e^b(N) \end{bmatrix}. \tag{3.56}$$

Using known relations, for a data matrix it is possible to display in types of expansion on singular numbers:

$$X_p^f = \sum_{n=1}^{p} \sigma_n^f u_n^f \left(v_n^f\right)^H,\ X_p^b = \sum_{n=1}^{p} \sigma_n^b u_n^b \left(v_n^b\right)^H, \tag{3.57}$$

where σ_n^f – positive singular numbers of the matrix X_p^f; σ_n^b – positive singular numbers of the matrix X_p^b; u_n and v_n – eigenvectors of the corresponding data matrices.

If the signal consists of a mixture of *m* exponents and additive noise, then *m* eigenvectors associated with *m* the most singular numbers will cover these exponential components. Rest *p–m* eigenvectors associated with smaller singular numbers will cover the noise components.

Assuming that the singular numbers are ordered in descending order, i.e. $\sigma_1^f > \sigma_2^f > \sigma_3^f \ldots > \sigma_p^f$, then it is possible to obtain a reduced approximation rank for each data matrix by cutting the relations for decomposition by singular numbers in (3.57) to *m* main singular numbers:

$$X_p^f = \sum_{n=1}^{m} \sigma_n^f u_n^f \left(v_n^f\right)^H, \; X_p^b = \sum_{n=1}^{m} \sigma_n^b u_n^b \left(v_n^b\right)^H. \tag{3.58}$$

This procedure will reduce the proportion of noise in the data matrix by increasing the signal-to-noise ratio.

Minimizing norms $\left\|a_p^f\right\|$ and $\left\|a_p^b\right\|$ relative to the reduced level data matrix, we obtain:

$$a_p^f = -\left(\widehat{X}_p^f\right) x_p^f, \; a_p^b = -\left(\widehat{X}_p^b\right) x_p^b. \tag{3.59}$$

In which pseudo-inverted matrices are defined by expressions:

$$\widehat{X}_p^f = \sum_{n=1}^{m} \left(\sigma_n^f\right)^{-1} v_n^f \left(u_p^f\right)^H, \; \widehat{X}_p^b = \sum_{n=1}^{m} \left(\sigma_n^b\right)^{-1} v_n^f \left(u_p^b\right)^H. \tag{3.60}$$

The value of the order *p* should lie in the interval $m \le p \le N - m$ for the rank of the matrices x_p^f, x_p^b was greater than or equal to *m* that is, a more predictable number of exponents. If the number of exponents is unknown, it can be estimated by comparison with the values of singular numbers. The singular numbers associated with the signal must be greater than the singular numbers associated with the noise. After obtaining the results of calculating the coefficients of linear prediction forward and backward, defined by expression (3.60), using the expressions (3.59) and (3.60) calculate the roots of the characteristic polynomials, which give estimates of the exponents. Data vectors x_p^f, x_p^b in the analysis of the effects of noise are not considered, despite the fact that they are noisy.

As a result of the methodical calculations, it is possible to detect noisy signals with a higher probability than the first determined method.

To consider the effect of interference on the signal, we assume that the interference is.

An obstacle – in our understanding, is any action that is imposed on external influences and makes it difficult to determine.

Depending on the source of the interference, all radio frequency interference that affects the existing information network can be divided into the following groups:

– atmospheric interference caused by electric discharges in the atmosphere;

– industrial barriers created by various electrical installations and power grids;

– fluctuation (any accidental) interference caused by fluctuation (accidental deviation) of electric current and voltage in circuits and electronic systems;

– space, created by radio radiation from the Sun and galaxies;

– contact interference due to the presence of time-varying contacts between the conductive surfaces that are in the zone of intense fields of the transmitters;

– mutual interference arising from the interaction of electromagnetic fields of any electronic means.

Obstacles can be intentional or unintentional. Intentional obstructions created specifically to hinder or disrupt the operation of the information transmission network. Intentional obstacles are divided into sighting and blocking. Unintentional obstacles include: mutual – from radio equipment; atmospheric (natural) – from various natural phenomena; local (industrial) – from local sources of interference. According to the intensity of the impact on radio communication, interference is divided into weak, strong and depressing. According to the degree of possibility of elimination of obstacles, obstacles can be classified as insurmountable and insurmountable.

In order to reduce the error that may affect the process of recognizing external influences, we define the main characteristics of the obstacle.

The main characteristic is the correlation function, which is defined by the expression:

$$K_x(\tau)=\overline{x}(t)\overline{x}(t+\tau)=\lim_{T\to\infty}\frac{1}{T}\int_0^T x(t)x(t+\tau)\mathrm{d}t. \qquad (3.61)$$

For the case of interference, and the recognition of signals of external influences – the physical meaning of the correlation function is as follows: $x(t)$ is detected energy spectrum of the impact signal, if at the time – t time value $x(t)$ is a definite quantity, it is unlikely that at the time $t+\tau$, where τ – very small, value $x(t+\tau)$ will be equal to zero. But if τ – will be taken large enough, the value $x(t+\tau)$ can be any. That is, between certain signals $x(t)$ та $x(t+\tau)$ there is a dependence that decreases with increasing τ. Behavior of probable magnitude $x(t)$ will be characterized not only by meaning but also by interrelationship $x(t)$ at time t and $x(t+\tau)$. A measure of this relationship is the correlation function.

The standard deviation will be determined by the expression:

$$\sigma^2(\tau)=\left[x(t)-x(t+\tau)\right]^2=2\left[K_x(0)-K_x(\tau)\right]. \qquad (3.62)$$

The standard deviation is completely determined by the correlation function, which indicates how much the two processes $x(t)$ and $x(t+\tau)$ are averaged.

All of the above is specific to the ergodic process. A stationary process is called ergodic in the narrow sense, if with a probability unit all its probabilistic characteristics can be obtained by one implementation of the process. Given that the different characteristics of the ergodic process are usually determined by averaging over time, we can say that a stationary random process is ergodic if the results of averaging over time coincide with the corresponding results of averaging over the set.

To further consider the interference that affects the signal of external influences, consider the main properties of the correlation function:

1. The correlation function of the ergodic signal is a pair function:

$$K_x(\tau)=K_x(-\tau). \qquad (3.63)$$

2. Any value of the correlation function cannot exceed the value of this function at zero value of the argument:

$$K_x(0) \geq K_x(\tau). \tag{3.64}$$

Let's prove this by considering the expression (3.60):

$$\sigma^2(\tau) = \left[x(t) - x(t+\tau)\right]^2 = 2\left[K_x(0) - K_x(\tau)\right] = 2K_x(0) - 2K_x(\tau).$$

It follows from this expression that it matters if:

$$2K_x(0) - 2K_x(\tau) \geq 0,\ K_x(0) \geq K_x(\tau),$$

which is a proof of the second property of the correlation function.

3. If the erosion process does not contain a deterministic component, then its correlation function coincides indefinitely with the growth of τ, with increasing dependence $x(t)$ and $X(t+\tau)$ decreases, when $\tau \to \infty$ they become independent. The presence of a deterministic component in the process $x(t) = \xi(t) + \xi_0$ lead to:

$$\lim_{\tau\to\infty} K_x = \lim_{\tau\to\infty}\left[\xi(t) + \xi_0\right] \times \left[\xi(t+\tau) + \xi_0\right] = \xi_0^2 = K(\infty). \tag{3.65}$$

4. The variance will be determined:

$$D\left[X(t)\right] = \sigma_x^2 - \xi_0^2 = K_x(0) - K_x(\infty). \tag{3.66}$$

5. The autocorrelation function of a periodic process is a periodic function with the period of this process.

Let's have a periodic process:

$$x(t) = a_0 + \sum_{k=1}^{\infty} a_k \cos(k\omega t + \varphi_k),$$

then bearing in mind the periodicity of $x(t)$ and taking the average for the period, we have:

$$K_x(\tau) = \frac{1}{T}\int_0^T \sum_{k=0}^{\infty}\sum_{n=0}^{\infty} a_k a_n \cos(k\omega t + \varphi_k)\cos\left(n\omega(t+\tau) + \varphi_n\right)dt. \tag{3.67}$$

Given that the integrals of the cosines at $k \neq n$ are equal to 0, and when $k = n \neq 0$, $1/2\cos k\omega\tau$, we'll get:

$$K_z(\tau) = a_0^2 + \sum_{k=1}^{\infty} \frac{a_k^2}{2}\cos k\omega\tau. \tag{3.68}$$

As we can see from expression (3.67), the correlation function does not depend on φ – phase harmonics of the initial signal, this is exactly what makes it possible to separate the signal from the interference.

Let $A(t)$ – a signal, $N(t)$ – obstacle, then we have: $X(t)=A(t)+N(t)$, define the correlation function:

$$K_x(\tau)=\left[A(t)+N(t)\right]\times\left[A(t+\tau)+N(t+\tau)\right]=K_A(\tau)+K_{AN}(\tau)+K_{NA}(\tau)+K_N(\tau),$$

where $K_A(\tau)$ – signal autocorrelation function; $K_N(\tau)$ – interference autocorrelation function; $K_{AN}(\tau)$, $K_{NA}(\tau)$ – intercorrelation function of interference and signal.

Given that the signal and interference are independent then:

$$K_{AN}(\tau)=0,\ K_{NA}(\tau)=0,$$

we have:

$$K_x(\tau)=K_A(\tau)+K_N(\tau). \tag{3.69}$$

To confirm the above, we model the function of the correlation processes described by expressions (3.68) and (3.69), depending on the change in signal frequency. The simulation results will be presented in the form of graphs. The obtained graphs are presented in **Fig. 3.8**, **Fig. 3.9**.

As can be seen from the graph shown in **Fig. 3.9**, the interference signals are much smaller, but they do not interfere with the detection of the impact signal itself and can be filtered.

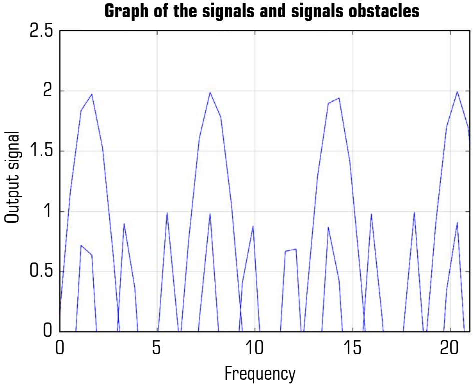
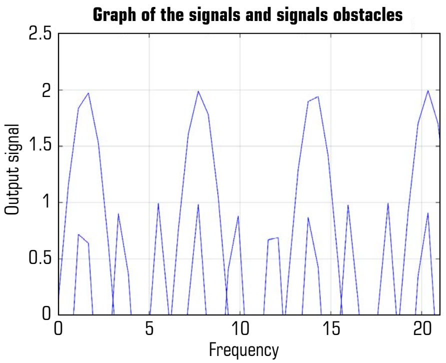


Fig. 3.8 Graph of the correlation function of the signal of information transmission over the network, without interference



⬡ **Fig. 3.9** Graph of the correlation function of the signal of information transmission over the network, with an obstacle

Thus, using the properties of the correlation function, it is possible to separate the signal from the interference. In the future, this method can be used for other non-periodic signals.

3.6 ASSESSING THE LEVEL OF ECONOMIC COSTS FOR THE PROTECTION OF INFORMATION IN THE SOCIAL NETWORK

Generalization of the model for assessing the level of protection of information in the social network from external influences on the information social resource is proposed to be carried out on the basis of the model of the level of protection of information in social networks. This model is described by the expression:

$$PR_{OZ}^{ISN} = \left\{\left\{I^{A}\right\},\left\{R^{ISN}\right\},\left\{IM^{ISN}\right\},\left\{RD^{ISN}\right\},\left\{SZ^{ISN}\right\},\left\{DAZ^{ISN}\right\},\left\{UZ^{ISN}\right\}\right\}, \tag{3.70}$$

where $\left\{I^{A}\right\}$ – set of elements of information in social networks; $\left\{R^{ISN}\right\}$ – set of elements of social networks users' reputation; $\left\{IM^{ISN}\right\}$ – set of sources of influence on the information security system; $\left\{RD^{ISN}\right\}$ – set of requirements of information security guidelines; $\left\{SZ^{ISN}\right\}$ – set of possible technical information security systems; $\left\{DAZ^{ISN}\right\}$ – set of security audit of information on social networks; $\left\{UZ^{ISN}\right\}$ – the level of information security in social networks.

Let's use the expression to define the connection between external influences and technical means of information protection:

$$V^{IMSZ} = \left\|v_{ij}^{IMSZ}\right\|. \tag{3.71}$$

It is necessary to take into account, more precisely, to take into account that the values *i* and *j* have a certain adjacent message, namely:

$$\forall i \in \{IM_k\} \text{ and } \forall j \in \{I^A\}. \tag{3.72}$$

The threat matrix will matter:

$$\left\|V^{IM}\right\| = \begin{cases} 1, \text{if there are } i \text{ impacts for } j\text{-th information active;} \\ 0, \text{ if there are not } i \text{ impacts for } j\text{-th information active.} \end{cases}$$

Every mechanism of information protection in social networks $SZ_k \in \{SZ^{ISN}\}$ characterized by a vector:

$$SZ_k = (T_{SZ}, T_v, C_{SZ}), \tag{3.73}$$

where T_{SZ} – type of information protection; T_v – implementation time; C_{SZ} – the cost of the protection system.

A matrix is used to describe the relationship between external influences and technical means of information protection:

$$V^{IMSZ} = \left\|v_{ij}^{IMSZ}\right\|, \tag{3.74}$$

where v_{ij}^{IMSZ} – reflects the existence of a link between the *i*-th impact on the information security system $IM_k \in \{IM^{ISN}\}$ and *j*-th technical means of information protection $SZ_k \in \{SZ^{ISN}\}$.

The model uses the following types of communication:

– *MZ* – protection mechanism that counteracts its destructive effect $VH_k \in \{VH\}$;

– *NMZ* – there is no protection mechanism to counter the *i*-th threat.

With $v_{ij}^{IMSZ} \in \{MZ, NMZ\}$, *MZ*, *NMZ* – there is a connection of a certain type between the *i*-th influence and the *j*-th technical means of information protection. For matrix elements, the values are determined by the rule:

$$\left\|v_{ij}^{IMSZ}\right\| = \begin{cases} MZ, \text{ if } i\text{-th influence is determined by } j\text{-th technical mean;} \\ MZ, \text{ if } i\text{-th influence isn't determined by } j\text{-th technical mean.} \end{cases}$$

If for all $i=m$, $v_{ij}^{IMSZ} = NMZ$, it is concluded that technical means of information protection in social networks are not able to protect information resources from a certain destructive impact, and therefore to increase the level of information security it is necessary to attract additional funds for protection mechanisms.

The next step is to determine the set of requirements of regulators $\{RD^{IMSZ}\}$, which consist of requirements for information protection in social networks – $\{R_{RD}\}$, specified in international and national recommendations, a set of assessments of the degree of compliance with security requirements $\{OV_{RD}\}$ and a set of final level of compliance of information protection in social networks $\{IU_{RD}\}$.

Then we have:

$$\left\{RD^{IMSZ}\right\}=\left\{R_{RD}\right\}\cup\left\{OV_{RD}\right\}\cup\left\{IU_{RD}\right\}. \tag{3.75}$$

Determination of the generalized indicator of the level of information security in the social network, which allows to assess the level of compliance of technical means of information protection with the requirements of the recommendations and documents:

$$OPZ^{ISN}=\sum_{i=1}^{k}OPZ_i, \tag{3.76}$$

where k – the number of individual indicators of information security.

OPZ_i – a single indicator acquires value from the set: OPZ_i – absence of unacceptable risks, at creation of system of protection of the information it is necessary to define models of threats. When compiling a threat model/attacker model and risk assessment (if unacceptable risks are identified, then $OPZ_i=0$, otherwise – $OPZ_i=1$).

OPZ_2 – absence of dangerous threats (if the detected threats are already blocked by technical means of information protection, then $OPZ_2=1$, if in the system of information protection in social networks, when compiling the model identified threats or influences that cannot be blocked by technical means of information protection existing system – $OPZ_2=0$).

OPZ_3 – the level of compliance of information security in the social network with the requirements of the recommendations for protection systems (if recognized as recommended – $OPZ_3=1$, if recognized as not recommended – $OPZ_3=0$).

Based on the data obtained, the system is assigned one of three levels of security:

$$UZ^{ISN}=\{\text{low, medium, high}\};$$

$$UZ^{ISN}=\begin{cases}\text{high if } OPZ^{ISN}=3;\\ \text{high if } 1\le OPZ^{ISN}\le 3;\\ \text{low if } OPZ^{ISN}=0.\end{cases} \tag{3.77}$$

The audit assessment of information security in the social network allows to determine the most valuable information assets of information, the effectiveness of the means used to protect them, as well as the degree of compliance of the technical protection system with protection requirements and the level of security, identify the most vulnerabilities and develop recommendations for improvement, if necessary, information security.

To assess the economic feasibility of implementing a mechanism of technical means of information protection in social networks, depending on the value of information, we introduce the following notation: V_S^{ISN} – the value of information for social network users (parties who own the information and try to protect it); V_S^{IZ} – value of information for the attacking party (trying to obtain information); SZ^{ISN} – means of possible technical means of information protection; $SV^{SN}=\left\{SV^{ISN},\ SV^{SNZ},\ SV^{SNZT}\right\}$ – funds allocated for obtaining information resources;

SV^{ISN} – means of hacking the mechanisms of the information access system; SV^{SNZ} – means of hacking the mechanisms of the information confidentiality system; SV^{SNZT} – means of breaking the mechanisms of technical means of information protection.

Based on the above we will have:

$$SV^{SN} = \left\{SV^{ISN}\right\} \cap \left\{SV^{SNZ}\right\} \cap \left\{SV^{SNZT}\right\}. \tag{3.78}$$

It is obvious that it is pointless to invest more in protecting or obtaining information than the value of the information itself. It doesn't make sense. That is, the correct inequalities:

$$V_S^{IZ} \geq SV^{SN}, \quad V_S^{SN} \geq SV^{ISN}. \tag{3.79}$$

To further develop the model of estimating economic costs, we assume that the probabilities are determined by the expressions:

$$P_{Zj} = \frac{q_Z \times SV^{ISN}}{q_Z \times SV^{SN} + q_V \times SV^{ISN}}, \tag{3.80}$$

$$P_{Vj} = \frac{q_Z \times SV^{ISN}}{q_Z \times SV^{SN} + q_V \times SV^{ISN}}, \tag{3.81}$$

where q_V, q_Z – weights that determine how close each side is to the goal; P_{Vj} – probability of realization of at least one *i*-th threat of the *j*-th asset (probability of success by the attacking party); P_{Zj} – probability of protection against the *i*-th threat of the *j*-th asset (the probability of success is protected by the party).

Assume that the amount of funds allocated by the attacking party is equal to the value of information, the value of information is the same for both parties, and the opposing parties are on equal terms, then the economic cost of information protection in social networks should not exceed:

$$SV^{ISN} = V_{IS}^{ISZ} \times \frac{\sqrt{5}-1}{2}. \tag{3.82}$$

Thus, the model of estimating economic costs for the information protection system in social networks has been improved. The effectiveness of the proposed model for estimating economic costs depends on the accuracy of formulating the probability of protection success and determining the value of information.

4 METHODOLOGICAL ASPECTS OF POSTQUANTUM ASYMMETRIC MCELIECE AND NIEDERREITER SYSTEMS ON ALGEBRA-GEOMETRIC CODES DESIGN

ABSTRACT

The practical aspects of the methodology for constructing post-quantum algorithms for asymmetric cryptosystems McEliece and Niederreiter on algebraic codes (elliptic and modified elliptic codes) and their mathematical models and practical algorithms are discussed. Hybrid crypto-code constructions (HCCC) of McEliece and Niederreiter on flawed codes are proposed, which can significantly (20 times) reduce energy costs for implementation, while ensuring the required level of cryptographic stability of the system in the post-quantum period. The concept of security of the corporate information and educational system (CIES) based on the construction of an adaptive information security system is proposed. To ensure the security of information resources of CIES, a model is proposed, which allows not only to take into account the synergy and hybridity of modern threats, but also to form preventive countermeasures.

KEYWORDS

Crypto-code constructions, post-quantum cryptosystems, modified codes, flawed codes.

The entry of mankind into the era of high technologies has made it possible to single out cyberspace (an abstract concept based on computer networks and Internet technologies) into a separate component of security and put it before information security and security of information. To ensure security, as a rule, symmetric cryptosystems with temporary strength are used, but fast (by 3–5 orders of magnitude) crypto transformations, in comparison with asymmetric cryptosystems that provide a provable level of security (strength is based on *NP*-complete problems), which allows them to be used in transmission key data of symmetric cryptosystems and form digital signature protocols (*DS*) providing the service of authenticity (authenticity of the message source). The rapid development of computing means provides a 2-fold increase in computing capabilities every 18 months, which significantly increases the scope of services in cyberspace. However, the analysis by US NIST specialists of traditional cryptography algorithms [122–124] and asymmetric cryptography algorithms, digital signature protocols (including algorithms using elliptic curves) showed that the computational capabilities in the post-quantum period are the use of full-scale quantum computers and the Grover and Shor hacking algorithms [125] – allow for polynomial time to break the cryptosystem data used in computer systems and networks of cyberspace, which casts doubt on the quality of providing basic security services: confidentiality, integrity and authenticity. In works [125–128] it is indicated that with the growth of computing capabilities, there is not only an expansion of IT services in almost all spheres of human activity, but also a significant increase in hybrid, providing a synergistic effect, target attacks with elements of social engineering. Thus, a scientific and technical problem arises to provide basic security services based on alternative approaches that ensure, first of all, the cryptographic strength of the algorithms used. Methods of digital steganography are another area that allows ensuring the secrecy of information circulation at critical infrastructure facilities. However, in works [129–133] practical algorithms for steganoanalysis are shown. Thus, the development of high technologies, the growth of computing resources, the possibility of the appearance of a full-scale computer put forward new more stringent requirements for the mechanisms for providing security services.

4.1 RESEARCH OF REQUIREMENTS FOR POST-QUANTUM CRYPTOGRAPHY ALGORITHMS

Analysis of recent research and publications [122–125, 134–138] showed that with the advent of a full-scale quantum computer, the security of modern cryptosystems providing basic security services is being questioned. Therefore, NIST USA specialists are holding a competition for post-quantum cryptography algorithms. Among the algorithms-contestants that passed to the second round there are also crypto-code constructions (CCC). Thus, the consideration of the use of the Niederreiter CCC on algebraic geometric codes (AGC) (codes on elliptic curves and/or their modifications, on defective codes) in practical algorithms of security services for their modification/improvement is an urgent task.

When implementing a full-scale quantum computer, Shor's algorithm allows factoring the number N into factors in the time $O(\lg_3 N)$ using $O(\lg N)$-bits register, which is significantly faster than any classical factorization method. The advantages of using quantum registers are significant memory savings (N quantum bits can contain $2N$ bits of information), the interaction between qubits makes it possible to affect the entire register in one operation (quantum parallelism).

Thus, Shor's algorithm called into question the very existence of asymmetric cryptography, since on its basis it is possible to effectively solve problems of discrete logarithm and other problems on the complexity of which cryptographic algorithms are based. This conclusion was confirmed in March 2018 in the report of the US NIST (Report on Post-Quantum Cryptography) [122, 123], which notes that the emergence of full-scale quantum computers casts doubts on the cryptographic strength of asymmetric cryptography algorithms, and in February 2019, experts NIST USA, at the opening of the competition for post-quantum cryptography algorithms, stated that the algorithms on elliptic curves are also being questioned. Thus, humanity enters the so-called post-quantum period – a period of time in the future when classical methods will be significantly improved and quantum computers with the register lengths (in qubits) necessary for successful cryptanalysis and the mathematical and software necessary for their implementation will be created. The main problems that can be solved on a quantum computer include the following:

1) Shor's quantum factorization algorithm;
2) quantum Grover's algorithm for finding an element in an unsorted base;
3) Shor's quantum algorithm for solving the discrete logarithm in a finite field;
4) quantum algorithm for solving the discrete logarithm in the eliptic curve (*EC*) Shor point group;
5) quantum cryptanalysis algorithms for transformations into factor ring;
6) quantum crypto analysis algorithm Xiong and Wang and its improvement and the like.

Table 4.1 shows the results of a comparative analysis of the complexity of factorization for classical and quantum algorithms, in **Table 4.2** – the complexity of the implementation of Shor's method of discrete logarithm to the group of eliptic curve (*EC*) points.

● **Table 4.1** Comparative analysis of the complexity of factorization for classical and quantum algorithms

Module size *N*, bit	Number of qubits required, 2*n*	Complexity of the quantum algorithm, $4n^3$	Complexity of the classical algorithm
512	1024	$0.54 \cdot 10^9$	$1.6 \cdot 10^{19}$
3072	6144	$12 \cdot 10^{10}$	$5 \cdot 10^{41}$
15360	30720	$1.5 \cdot 10^{13}$	$9.2 \cdot 10^{80}$

● **Table 4.2** The complexity of the implementation of Shor's method of discrete logarithm to the point group *EC*

Base point order size, bit	Number of qubits required $f(n)=7n+4\log_2 n+10$	Complexity of the quantum algorithm $360n^3$	Complexity of the classical algorithm
163	1210	$1.6 \cdot 10^9$	$3.4 \cdot 10^{24}$
256	1834	$6 \cdot 10^9$	$3.4 \cdot 10^{38}$
571	4016	$6.7 \cdot 10^{10}$	$8.8 \cdot 10^{85}$
1024	7218	$3.8 \cdot 10^{11}$	$1.3 \cdot 10^{154}$

Presented in **Tables 4.1**, **4.2**, the results of comparisons indicate a significant reduction in energy costs for the implementation of breaking cryptoalgorithms of asymmetric cryptography, which include DS algorithms when using a quantum computer, which significantly reduces the level of «trust» in algorithms and protocols for providing basic security services: confidentiality, integrity and authenticity.

In the conditions of post-quantum cryptography, NIST experts suggest considering attacks of a special type (SIDE-CHANEL ATTACKS). The implementation of these attacks is aimed at finding vulnerabilities in the practical implementation of the cryptosystem, primarily the means of cryptographic protection.

The following classification of special attacks based on the following features was proposed:

– control of the computing process;

– the way to access the system or tool;

– the method of direct attack and the like.

Protection against special attacks can be based on features:

– fixed number of calls to the hash function, data randomization;

– independence of keys from values and the like.

The main NIST requirements for safety in the post-quantum period are:

1. Safety requirements:

– replacement of the ES standard FIPS 186;

– replacement of key distribution standards SP 800-56A, SP 800-56B;

– using the new standard in protocols: TLS, SSH, IPSec etc.;

– security model for encryption and distribution is a «semantically secure encryption» scheme;

– security model – IND-CCA2.

2. Safety conditions:

– attacker access to less than 2^{64} selected ciphertext-key pairs.

3. Resilience requirements:

– 128-bit classic security/64-bit quantum security (AES-128 security margin);

– 128-bit classic security/80-bit quantum security margin (SHA-256/SHA3-256, SHA-384/SHA3-384);

– 256-bit classic security/128-bit quantum security (AES-256 security margin).

Thus, NIST USA suggests considering the following models:

– for symmetric cryptography algorithms – under the conditions of the security model IND-CCA2 (Indistinguishability Adaptive Ciphertext Attack), which determines the resistance to an adaptive attack based on the selected text cipher;

– for electronic digital signature – under the conditions of the security model EUF-CMA (existentially unforgeable under adaptive chosen message attacks);

– for the key encapsulation protocol – under the conditions of the security model Canetti-Krawczyk (CK-security).

As a preliminary criterion, NIST proposes an approach in which quantum attacks are limited to a set of fixed runtimes, or «depths», of the scheme. This parameter is named MAXDEPTH.

Possible values for the range MAXDEPTH:

– 240 logical gates, that is, the approximate number of gates that will be sequentially executed per year;

– 264 logic gates that modern classical computing architectures can execute sequentially in ten years;

– not more than 296 logical gates, that is, an approximate number of gates, how atomic-scale qubits with the speed of light propagation time can perform over millennia.

Thus, the analysis showed that the use of EDS based on asymmetric cryptoalgorithms in the post-quantum period cannot provide a guaranteed level of cryptographic strength, and, accordingly, can be subject to a special type of attack based on a full-scale quantum computer.

4.2 PROPERTIES OF ASYMMETRIC CRYPTO-CODE SYSTEMS MCELIECE AND NIEDERREITER BASED ON ELLIPTICAL CODES

To provide security services, standards based on symmetric and asymmetric cryptography are generally used. It is known that symmetric cryptographic algorithms belong to the model of practical stability, provide ease of implementation and encryption speed 3–5 orders higher than asymmetric ones. Asymmetric cryptographic algorithms provide evidence-based stability. However, under the conditions of post-quantum cryptography, the cryptographic strength of traditional cryptography and public-key cryptography algorithms, including elliptic curve algorithms, is called into question. NIST experts consider crypto-code constructions to be one of the promising areas of post-quantum cryptography algorithms.

Their use allows combining the advantages of symmetric and asymmetric cryptosystems and additionally ensuring the reliability of the transmitted information based on the use of noise-resistant coding, that is, use transmission with direct error correction.

Fig. 4.1 shows the classification of crypto-code constructions.

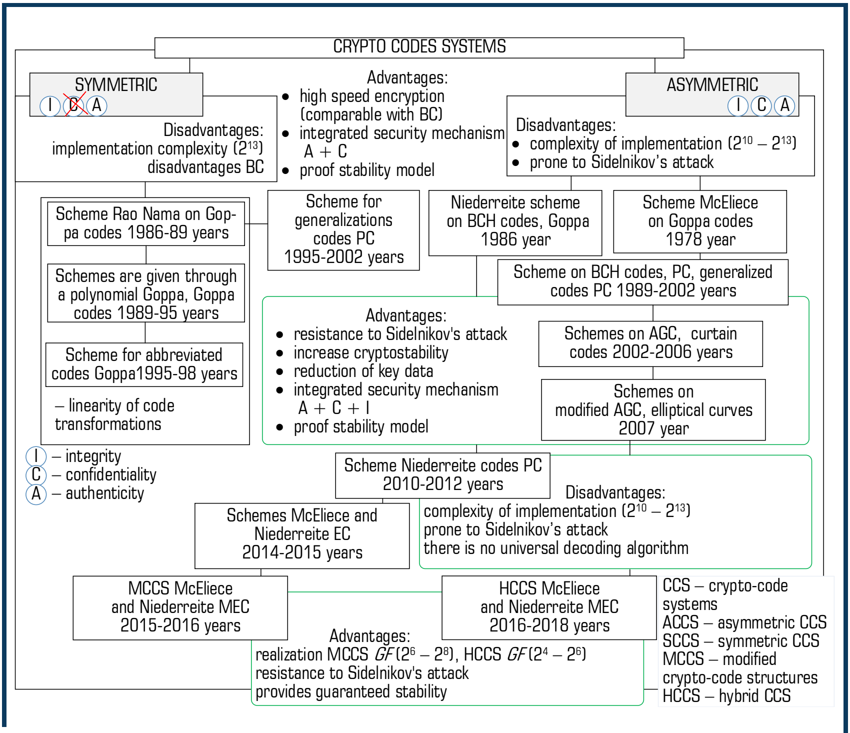

CRYPTO CODES SYSTEMS
SYMMETRIC
I C A
Advantages:
• high speed encryption (comparable with BC)
• integrated security mechanism A + C
• proof stability model
ASYMMETRIC
I C A
Disadvantages:
implementation complexity (2^{13})
disadvantages BC
Disadvantages:
• complexity of implementation ($2^{10} – 2^{13}$)
• prone to Sidelnikov's attack
Scheme Rao Nama on Goppa codes 1986-89 years
Scheme for generalizations codes PC 1995-2002 years
Niederreite scheme on BCH codes, Goppa 1986 year
Scheme McEliece on Goppa codes 1978 year
Schemes are given through a polynomial Goppa, Goppa codes 1989-95 years
Scheme on BCH codes, PC, generalized codes PC 1989-2002 years
Advantages:
• resistance to Sidelnikov's attack
• increase cryptostability
• reduction of key data
• integrated security mechanism A + C + I
• proof stability model
Schemes on AGC, curtain codes 2002-2006 years
Scheme for abbreviated codes Goppa1995-98 years
Schemes on modified AGC, elliptical curves 2007 year
– linearity of code transformations
I – integrity
C – confidentiality
A – authenticity
Scheme Niederreite codes PC 2010-2012 years
Disadvantages:
complexity of implementation ($2^{10} – 2^{13}$)
prone to Sidelnikov's attack
there is no universal decoding algorithm
Schemes McEliece and Niederreite EC 2014-2015 years
MCCS McEliece and Niederreite MEC 2015-2016 years
HCCS McEliece and Niederreite MEC 2016-2018 years
Advantages:
realization MCCS $GF(2^6 – 2^8)$, HCCS $GF(2^4 – 2^6)$
resistance to Sidelnikov's attack
provides guaranteed stability
CCS – crypto-code systems
ACCS – asymmetric CCS
SCCS – symmetric CCS
MCCS – modified crypto-code structures
HCCS – hybrid CCS

Fig. 4.1 Classification of crypto-code constructions

The analysis carried out in works [104, 134–144] showed that these cryptosystems allow providing a provable (mathematically) level of security (strength is based on the NP-complete problem – decoding a random code), ensure the efficiency of crypto transformations at the level of encryption speed with traditional cryptography algorithms and reliability, due to the use of error-correcting codes. In addition, the report of NIST specialists [122, 124] noted that it is crypto-code constructions that allow providing the required level of cryptographic strength in post-quantum cryptography.

The known methods of their construction on the basis of noise-resistant (algebraic geometric codes, AGK), mathematical models and practical algorithms are considered in works [104, 124, 134–144].

Based on McEliece's crypto-code construction, first proposed in [144]. As a secret (private key), the generating matrix of the linear (n, k, d) code on $GF(q)$ – G, and *masking matrices:* non-degenerate $k \times k$-matrix on $GF(q)$ – X, diagonal $n \times n$-matrix D, permutation $n \times n$-matrix – P.

The permutation matrix implements the permutation of vector coordinates in the form of matrix multiplication. The public key is the matrix $G_X=X\times G\times P\times D$.

Encryption:

$$A_X^* = i \times G_X + e,$$

where vector $c_X=i\times G_X$ belongs to (n, k, d) code with the generator matrix G_X; i – k-bit information vector; vector e – error vector of weight $\leq t$, serves as an additional secret parameter (session key).

On the receiving side, the receiver, knowing the public key, and using the Berlekemp-Messi decoding algorithm (polynomial complexity), receives the original text. The exchange protocol between authorized users based on the McEliece crypto-code construction (CCC) on algebraic geometric (elliptic, *EC*) codes is shown in **Fig. 4.2**.

To eliminate the drawback – the Sidelnikov attack implementation, it is proposed to use algebraic geometric codes, codes built on curves (as an example, on elliptic curves).

Singular (supersingular) curves of 3 kinds are used to form the AGC (*EC*).

Algebrogeometric code along the curve X over $GF(q)$ – this is a linear code of length $n \leq N$, code words $C(c_1,c_2,\ldots,c_n)$ of which are given by the equality:

$$\sum_{i=0}^{k-1} i_j F_j\left(P_i\right) = c_i,$$

where $P_i(X_i,Y_i,Z_i)$ – projective points of the curve X, i.e. (X_i,Y_i,Z_i) – solutions of a homogeneous algebraic equation defining the curve X, $i=\overline{1,n}$; $F_j\left(P\right)_i$ – values of the generator functions at the points of the curve.

This definition is equivalent to the matrix representation of the algebraic geometric code [125]:

$$G\left(i_0, i_1, \ldots, i_{k-1}\right)^T = \left(c_0, c_1, \ldots, c_{n-1}\right),$$

where G – generator matrix of dimension $k\times n$, $k=\alpha-g+1$, $\alpha=degX\times degF$ of view:

$$G = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \ldots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \ldots & F_1(P_{n-1}) \\ \ldots & \ldots & \ldots & \ldots \\ F_{k-1}(P_0) & F_{k-1}(P_1) & \ldots & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j\left(P_i\right) \right\|_{n,k}.$$

However, the construction of the CCC on *EC* does not eliminate the disadvantage of significant energy consumption in practical implementation. To eliminate the disadvantage, it is proposed to use modified *EC* (*MEC*), proposed in works [104, 135, 137].

Consider a *cryptosystem based on Niederreiter's crypto-code construction*, first proposed in [145]. Private (private) key check matrix H-linear (n, k, d) code on $GF(q)$, *masking matrices:* non-degenerate $r\times r$-matrix on $GF(q)$ – X, diagonal $n\times n$-matrix D, permutation $n\times n$-matrix – P. Opened (public) key matrix $H_X=X\times H\times P\times D$.

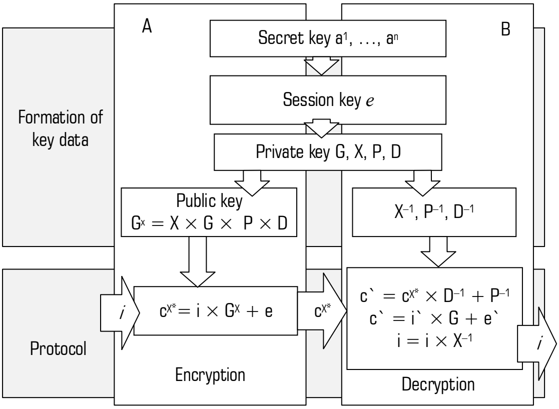


Fig. 4.2 Protocol in an asymmetric cryptosystem based on the McEliece CCC

Rule encryption:

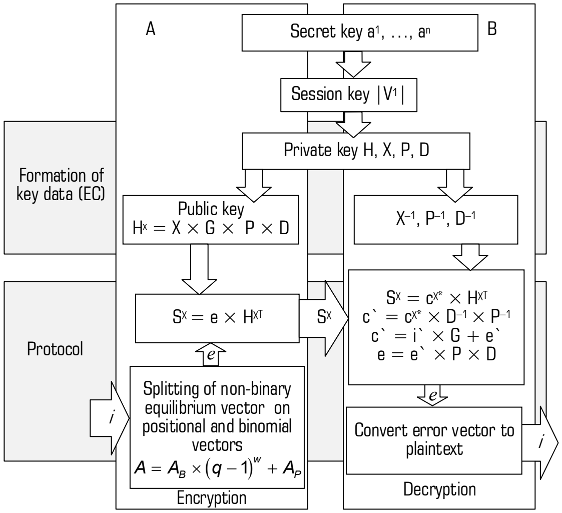
$$S_X = e \times H_X^T,$$

where vector e – is a vector of length n and weight $\leq t$, is computed in advance based on the equilibrium coding and is a transformed input sequence. On the receiving side, the recipient finds from q^k solutions of expression $S_X = A_X^* \times H_X^T$. Next, decryption is used based on the Berlekamp-Messi algorithm.

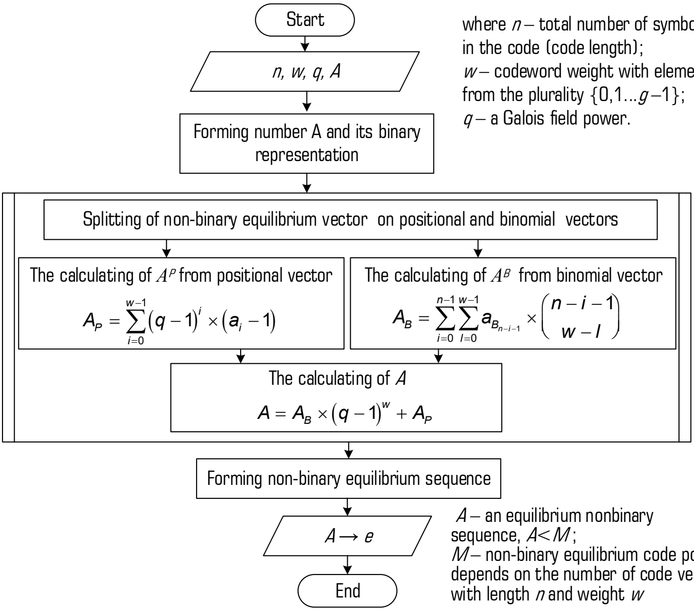
The scheme of the exchange protocol in an asymmetric cryptosystem based on the Niederreiter crypto-code construction on elliptic codes is presented in the form of **Fig. 4.3**. To use the EC in the Niederreiter CCC, the equilibrium coding of m-ary codes is used – the block diagram of the algorithm is shown in **Fig. 4.4**. To form a cryptogram at the first stage, the plaintext is converted into an error vector based on the equilibrium coding algorithm. After this, a syndrome is formed by multiplying the check matrix on elliptic codes by an error vector. Practical implementation of the scheme showed that when using elliptic codes, it is necessary to take into account positional clear-text sets {MF} for «sifting out» error vector sets that do not allow using the classical version of decoding information on the receiving side.

Elements of positional sets form a session key and allow to increase the level of cryptographic stability. **Fig. 4.5** shows an encryption algorithm in the Niederreiter CCC in the EC.

The analysis showed that for the provision of basic security services**,** crypto code constructions are usually used based on the McEliece and Niederreiter schemes. To ensure the level of cryptographic strength in post-quantum cryptography, it is necessary to use the power of the alphabet in a field of 2^{10}–2^{13} degrees, which is a significant drawback of their practical application. Even at the current level of computer technology, this is a rather difficult task.


A
Secret key $a^1, \ldots, a^n$
B
Session key $|V^1|$
Private key H, X, P, D
Formation of key data (EC)
Public key
$H^x = X \times G \times P \times D$
X^{-1}, P^{-1}, D^{-1}
Protocol
$S^x = e \times H^{xT}$
S^x
$S^x = c^{x*} \times H^{xT}$
$c` = c^{x*} \times D^{-1} \times P^{-1}$
$c` = i` \times G + e`$
$e = e` \times P \times D$
e
i
Splitting of non-binary equilibrium vector on positional and binomial vectors
$A = A_B \times (q-1)^w + A_P$
e
Convert error vector to plaintext
i
Encryption
Decryption

⬡ **Fig. 4.3** An exchange protocol in an asymmetric cryptosystem based on the Niederreiter CCC on the *EC*


Start
n, w, q, A
Forming number A and its binary representation
Splitting of non-binary equilibrium vector on positional and binomial vectors
The calculating of A^P from positional vector
$A_P = \sum_{i=0}^{w-1} (q-1)^i \times (a_i - 1)$
The calculating of A^B from binomial vector
$A_B = \sum_{i=0}^{n-1} \sum_{l=0}^{w-1} a_{B_{n-i-1}} \times \binom{n-i-1}{w-l}$
The calculating of A
$A = A_B \times (q-1)^w + A_P$
Forming non-binary equilibrium sequence
$A \to e$
End

where n – total number of symbols in the code (code length);
w – codeword weight with elements from the plurality $\{0,1\ldots g-1\}$;
q – a Galois field power.

A – an equilibrium nonbinary sequence, $A<M$;
M – non-binary equilibrium code power depends on the number of code vectors with length n and weight w

⬡ **Fig. 4.4** Algorithm of the equilibrium coding *EC* in the crypto-code construction of the Niederreiter

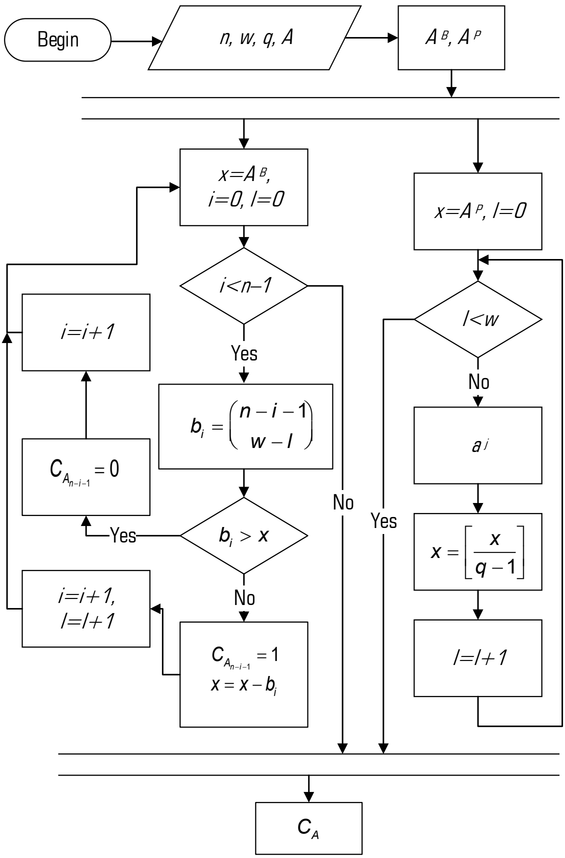


Fig. 4.5 CCC encryption algorithm on the *EC*

The second drawback is the hacking attack of the McEliece scheme based on linear-fractional transformations and the property of triply transitivity of the automorphism group of the generalized Reed-Solomon code, proposed in the work of professor of Sidelnikov from Moscow State University. The essence of attack is to find the elements of the generating matrix and remove the action of masking matrices. The orthogonality of the matrices, which is generative and test, allows us to consider the effectiveness of the attack on the Niederreiter scheme. A promising way to eliminate the identified patterns Sidelnikov proposes to use cascade or algebraic geometry codes – codes built on the basis of the algebra of the theory of noise-resistant coding and geometric parameters of the curve, in particular elliptic curves.

4.3 SIDELNIKOV'S ATTACK ON THE CRYPTO-CODE CONSTRUCTIONS OF MCELIECE AND NIEDERREITER

When considering the cryptanalysis algorithm for code-theoretic schemes and studying the properties of linear fractional transformations used in this case, we will use the main theoretical results given in [139, 140].

Elements of the group of linear fractional transformations $\varphi(x)$ are linear fractional functions:

$$\varphi(x)=\frac{ax+b}{cx+d},$$

other than constant, i.e. functions for which the determinant of the matrix:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

nonzero, $a, b, c, d \in GF(q)\cup\{\infty\}=F_q$.

Each fractional linear transformation $\varphi(x)$ one-to-one displays a set of elements F_q into itself. Group $\varphi(x)$ is non-commutative with group operation:

$$\varphi(x)\oplus\varphi'(x)=\varphi(\varphi'(x)x)$$

and has order:

$$(q+1)q(q-1).$$

The main property of the group $\varphi(q)$, used in [139] for effective cryptanalysis (removing the action of masking matrices) of code-theoretic schemes on generalized Reed-Solomon codes), consists in triple transitivity $\Phi(q)$ [139]. This means that for any two pairs (a_1, a_2, a_3) and (b_1, b_2, b_3), $a_i, b_i \in F_q$, with pairwise different coordinates in $\varphi(q)$ there is one element φ, for which it is true $\varphi(a_i)=b_i$, $i=1, 2, 3$. Moreover, the automorphism group G_q generalized Reed-Solomon code contains a subgroup isomorphic to the group of linear fractional transformations $\Phi(q)$ [139].

Group of automorphisms G_q generalized Reed-Solomon code is also thrice-transitive: for any pair of ordered triples $(\beta_1, \beta_2, \beta_3)$ and $(\gamma_1, \gamma_2, \gamma_3)$ with pairwise different coordinates, where $\{\beta_1, \beta_2, \beta_3\}, \{\gamma_1, \gamma_2, \gamma_3\}\in\{\alpha_1, \alpha_2, \ldots, \alpha_n\}=GF(q)\cup\{\infty\}$, there exists a monomial (with one nonzero element in each row and in each column) matrix $\Lambda_\varphi \in G_q$, which translates three coordinates $(x_{\beta_1}, x_{\beta_2}, x_{\beta_3})$ of the vector $x=(x_{\alpha_1}, x_{\alpha_2}, \ldots, x_{\alpha_n})$ into coordinates $(x_{y_1}, x_{\gamma_2}, x_{\gamma_3})$ of the vector $x\,\Lambda_\varphi$ multiplying them by the corresponding constants determined by the eigenvalues and matrices $\Lambda_\varphi \in G_q$.

Using the considered properties of the triple transitivity of the automorphism group G_q of the generalized Reed-Solomon code and the group of linear fractional transformations in [139, 140] it was shown that applying the corresponding function $\varphi(x)$ you can move any three coordinates of the vector to the first three places $x=(x_{\alpha_1}, x_{\alpha_2}, \ldots, x_{\alpha_n})$. Calculating the first three coordinates of the vector $x=\left(x_{\alpha_1},x_{\alpha_2},\dots,x_{\alpha_n}\right)$ in [139], proposed a polynomial algorithm for calculating the entire vector $x=\left(x_{\alpha_1},x_{\alpha_2},\dots,x_{\alpha_n}\right)$, which is the main part of the secret key of a code-theoretic scheme based on generalized Reed-Solomon codes. Thus, the property of three times transitivity of a group by an automorphism of generalized Reed-Solomon codes and a group of linear fractional transformations underlies the corresponding cryptanalysis method. Cryptosystems built on codes that are free of the indicated properties of a group of automorphisms are not vulnerable to such cryptanalysis – only those that are built using non-cyclic coding methods (which do not allow a polynomial description over a polynomial ring in one formal variable) can be considered potentially stable code-theoretic schemes that allow algebraically to define extensive classes of codes with arbitrary parameters and take arbitrary length over a finite alphabet of symbols [139]. Algebraic geometric codes are considered to be a promising direction in this sense.

Indeed, as shown in [104, 125, 137, 142, 143], algebraic geometric codes in the general case are noncyclic and are defined in terms of a linear system arising on algebraic curves. A linear system is specified by mapping the points of a curve to a projective space of a fixed dimension. The papers [137, 142, 143] give examples of the practical construction of algebraic geometric codes on curves. The use of algebraic geometric codes, as will be shown below, makes it possible to effectively build cryptographic means of protecting information with high structural properties.

4.4 ASYMMETRIC CRYPTO-CODE CONSTRUCTIONS OF MCELIECE AND NIEDERREITER BASED ON MODIFIED ELLIPTICAL CODES

To reduce energy costs and the practical implementation of crypto-code constructions without reducing the level of cryptographic strength of the system as a whole, it is proposed to use modified crypto-code constructions (MCCC) on modified (shortened and/or elongated) elliptic codes. It is the parameter *d* that provides cryptographic stability; therefore, to ensure cryptographic stability, it is necessary to fix it, which determines the use of modification methods with a fixed value of the structural-code distance, i.e. lengthening and shortening the code word. The **Fig. 4.6** demonstrates the features of modified shortened and elongated codes depending on their construction.

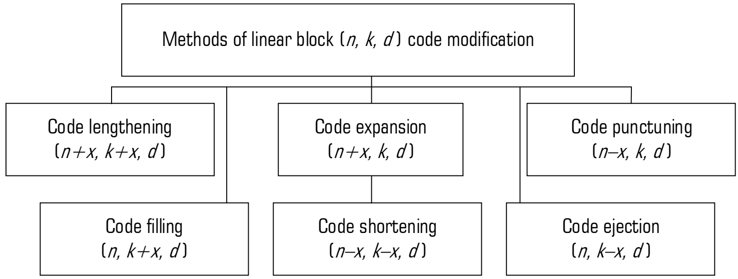

Methods of linear block (*n*, *k*, *d*) code modification
Code lengthening ($n+x$, $k+x$, d)
Code expansion ($n+x$, k, d)
Code punctuning ($n–x$, k, d)
Code filling (n, $k+x$, d)
Code shortening ($n–x$, $k–x$, d)
Code ejection (n, $k–x$, d)

Fig. 4.6 Methods for modifying error-correcting codes

The simplest and most convenient method of modifying a linear block code, not reducing the minimum code distance is shortening its length by reducing the information symbols. Let $I=(I_1,I_2,\dots,I_k)$ – information vector (n, k, d) of block code. We chose a subset h of information symbols, $|h|=x$, $x\leq 1/2k$. We put zeros in the information vector I in the subset h, i.e. $I_i=0$, $\forall I_i\in h$. On the other positions of the vector I, we place the information symbols. While the information vector encoding, the symbols of the set h are not involved (they are null) and can be discarded, and the resulting code word is shorter by x code symbols. For modification (shortening) of elliptic codes, we use the reduced set of the curve points. The following statement is true.

Statement 1. Let EC – an elliptic curve over $GF(q)$, $g=g(EC)$ – the curve genus, $EC(GF(q))$ – a set of its points over a finite field, $N=EC(GF(q))$ – their number. Let X and h – nonintersecting subsets of points, $X\cup h=EC(GF(q))$, $|h|=x$. Then *shortened* elliptic (n, k, d) code over $GF(q)$, built through mapping like φ: $X\to P^{k-1}$, is linked by characteristics $k+d\geq n$, where:

$$n = 2\sqrt{q} + q + 1 - x,\ \ k \geq \alpha - x, \tag{4.1}$$

$$d \geq n - \alpha, \alpha = 3\deg F.$$

Statement 2. *Shortened* elliptic (n, k, d) code over $GF(q)$, built through mapping like φ: $X\to P^{r-1}$, is linked by characteristics $k+d\geq n$, where:

$$n = 2\sqrt{q} + q + 1 - x,\ \ k \geq n - \alpha, \tag{4.2}$$

$$d \geq \alpha,\ \ \alpha = 3\deg F.$$

Second method for modifying a linear block code, which stores the minimum code distance and increases the amount of data transmitted is the elongation of its length after forming initialization vector, by reducing the information symbols. Let $I=(I_1,I_2,\dots,I_k)$ – information vector of (n, k, d) block code. Choose a subset h of the information symbols, $|h|=x$, $x\leq 1/2k$ and form *initialization vector*.

An information vector I in a subset of zeros h, i.e. $I_i=0$, $\forall\ I_i\in h$. On the other positions of the vector I put the information symbols. After in position of initialization vector add information symbols. For the modification (lengthening) elliptic codes will use reduction of the curve points multiplicity. The following statement is true.

Statement 3. Let EC – elliptic curve over $GF(q)$, $g=g(EC)$ – curve genus, $EC(GF(q))$ – multiplicity of its points over a finite field, $N=EC(GF(q))$ – their number. Fix a subset $h_1\subseteq h$, $|h_1|=x_1$. Let an elliptic (n, k, d) code over $GF(q)$ built through a mapping in the form φ*:* $X\to P^{k-1}$ is given. Then the parameters of the elongate on x_1 symbols from $GF(q)$ elliptic code built through mapping φ: $(X\cup h_1)\to P^{k-1}$, are related as follows: $k\geq\alpha-x+x_1$, $d\geq n-\alpha$, $\alpha=3\times degF$.

Evidence. If $x_1<x$, then the lengthening code on x_1 is equivalent to shortening the source code on the $x-x_1$. Having substituted these parameters in the expression, we obtain the result of corollary 1.

Corollary 1. The volume of private key (in bits) in motivated crypto-code system based on the theoretical-code McEliece scheme built on elliptical (n, k, d) code over $GF(2^m)$ is determined by the sum of matrix elements X, P, D (in bits), and is given by:

$$l_{K+} = 5 \times n^2 \times k^2 \times m. \tag{4.3}$$

Evidence. Indeed, secret key in McEliece scheme-generating matrix A (generating code matrix) and masking matrix X, P, D. In order to determine private key (in bits) of an elliptic (n, k, d) code over $GF(2^m)$, according to 1, it is sufficient to define multiplicity of coefficients $a_1 \ldots a_6$, $\forall a_i \in GF(2^m)$, and elements of masking matrixes. Total must be stored $l_{K+} = 5 \times n^2 \times k^2 \times m$ bits of secret key information [125].

Corollary 2. If you know the type of elliptic curve (multiplicity $a_1 \ldots a_6$, $\forall a_i \in GF(q)$), the subset of h and h_1 are completely determine the modified elliptical (n, k, d) codes over $GF(q)$, built through the mapping of the form: φ: $X \rightarrow P^{k-1}$ and φ: $(X \cup h_1) \rightarrow P^{k-1}$.

Evidence. Multiplicity of coefficients $a_1 \ldots a_6$, $\forall a_i \in GF(q)$ is uniquely defined form of the elliptic curve, and, accordingly, multiplicity of its points $EC(GF(q))$. Using a mapping in the form of φ: $EC \rightarrow P^M$ and the results of statements 3, construct the elliptical (n, k, d) code over $GF(q)$. If you know the elongating symbols, then we construct the elongated codes.

According to the statement 3, it is symbols from multiplicity h_1, which completely determine the modified elliptical (n, k, d) code over $GF(q)$.

Statement 4. Fix a subset $h_1 \subseteq h$, $|h_1| = x_1$. Let an elliptic (n, k, d) code over $GF(q)$, built through a mapping of the form φ: $X \rightarrow P^{r-1}$ is given. Then the elliptic code parameters of the elongated on x_1 characters from $GF(q)$, built by mapping of the form φ: $(X \cup h_1) \rightarrow P^{r-1}$, will be connected by the relations: $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \times degF$.

Corollary 3. If you know the form of an elliptic curve (multiplicity $a_1 \ldots a_6$, $\forall a_i \in GF(q)$), the subset of h and h_1 completely determine the modified elliptical (n, k, d) codes (*MEC*) over $GF(q)$, built through the mapping of the form: φ: $X \rightarrow P^{r-1}$ and φ: $(X \cup h_1) \rightarrow P^{r-1}$.

Evidence. The multiplicity of coefficients $a_1 \ldots a_6$, $\forall a_i \in GF(q)$ uniquely defines form of an elliptic curve, and, accordingly, multiplicity of its points $EC(GF(q))$. Using a mapping of the form φ: $EC \rightarrow P^M$ and results of statements 3, 4, construct an elliptic (n, k, d) code over $GF(q)$. If you know the lengthening symbols, then we construct the elongated codes. According to the statement 3, the symbols of the multiplicities h and h_1, which completely determine the modified elliptical (n, k, d) code over $GF(q)$.

Results of statements 3, 4, and their corollaries allow us to construct modified (elongated) elliptical (n, k, d) codes over $GF(q)$. Define the following algorithm for constructing modified elliptic codes.

Mathematical model of asymmetric crypto-code systems (ACCS) using the McEliece CCC based on shortening (*reduction of information symbols*) is formally defined by a combination of the following elements [125]:

– a set of plaintexts $M = \left\{M_1, M_2, \ldots, M_{q^k}\right\}$, where $M_i = \left\{I_0, I_{h_1}, \ldots I_{h_j}, I_{k-1}\right\}$, $\forall I_j \in GF(q)$, h_j – information symbols equal to zero, $|h| = 1/2k$, i. e $I_i = 0$, $\forall I_i \in h$;

– a set of secret texts (*codegrams*) $C = \left\{C_1, C_2, \ldots, C_{q^k}\right\}$, where $C_i = \left(A^*_{X_0}, A^*_{h_1}, \ldots, A^*_{h_j}, A^*_{X_{n-1}}\right)$, $\forall A^*_{X_j} \in GF(q)$;

– a set of direct mappings (based on public key usage – generating matrix) $\varphi = \left\{\varphi_1, \varphi_2, \ldots, \varphi_s\right\}$, where $\varphi_i : M \to C_{k-h_j}$, $i = 1,2,\ldots,s$;

– a set of inverse mappings (based on secret (private) key usage –disguise matrixes) $\varphi^{-1} = \left\{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_s^{-1}\right\}$, where $\varphi_i^{-1} : C_{k-h_j} \to M$, $i = 1,2,\ldots,s$;

– a set of keys, parameterizing direct mappings (public key of the authorized user) $K_{a_i} = \left\{K_{1_{a_i}}, K_{2_{a_i}}, \ldots, K_{s_{a_i}}\right\} = \left\{G_{Xa_i}^{EC_1}, G_{Xa_i}^{EC_2}, \ldots, G_{Xa_i}^{ECs}\right\}$, where $G_{Xa_i}^{EC_i}$ – generating $n \times k$ matrix disguised as a random code of algebra-geometric block (n, k, d) code with elements from $GF(q)$, i.e. $\varphi_i : M \xrightarrow{K_{ia_i}} C_{k-h_j}$; $i = 1,2,\ldots,s$; a_i – a set of polynomial curve coefficients $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, uniquely defining a specific set of points on the curve from the space P^2;

– a set of keys, parameterizing inverse mappings (private (secret) key of the authorized user) $K^* = \left\{K_1^*, K_2^*, \ldots, K_s^*\right\} = \left\{\left\{X,P,D\right\}_1, \left\{X,P,D\right\}_2, \ldots, \left\{X,P,D\right\}_s\right\}$, $\left\{X,P,D\right\}_i = \left\{X^i, P^i, D^i\right\}$, where X^i – disguise nondegenerate randomly equiprobably formed by a source of keys $k \times k$ matrix with elements from $GF(q)$; P^i – permutation randomly equiprobably formed by a source of keys $n \times n$ matrix with elements from $GF(q)$; D^i – diagonal formed by a source of keys $n \times n$ matrix with elements from $GF(q)$; i.e. $\varphi_i^{-1} : C \xrightarrow{K_i^*} M$, $i = 1,2,\ldots,s$, the complexity of the inverse mapping φ_i^{-1} without knowing the key $K_i^* \in K^*$ is associated with solving theoretical-complexity problems in random code decoding (general position code).

The initial data in the description of the considered asymmetric crypto-code information protection system are:

– algebrogeometric block (n, k, d) code C_{k-h_j} over $GF(q)$, i.e. a set of code words $C_i \in C_{k-h_j}$ such that the equality is true $C_i H^T = 0$, where H – check matrix of algebrogeometric block code;

– a_i– a set of the curve polynomial coefficients $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, uniquely defining a specific set of the curve points from space P^2 to form the generating matrix;

– h_j –information symbols, equal to zero, $|h| = 1/2k$, i.e. $I_i = 0$, $\forall I_i \in h$;

– disguising matrix mappings, given by a set of matrices $\left\{X, P, D\right\}_i$.

In asymmetric crypto-code system based on the McEliece CCC, the modified (shortened) algebrogeometric (n, k, d) code C_{k-h_j} with fast decoding algorithm is disguised as a random (n, k, d) code $C_{k-h_j}^*$ by multiplying the generating matrix G^{EC} of the code C_{k-h_j} by the secret disguise matrices X^u, P^u and D^u [4], providing the formation of the authorized user's public key: $G_X^{ECu} = X^u \times G^{EC} \times P^u \times D^u$, $u \in \left\{1,2,\ldots,s\right\}$.

Forming a closed text $C_j \in C_{k-h_j}$ on the basis of the entered plaintext $M_i \in M$ and a given public key $G_{Xa_i}^{ECu}$, $u \in \left\{1,2,\ldots,s\right\}$ is carried out by forming a code word of the disguised code by adding a random vector $e = \left(e_0, e_1, \ldots, e_{n-1}\right)$:

$$C_j = \varphi_u\left(M_i, G_X^u\right) = M_i \times \left(G_X^u\right)^T + e,$$

where the Hamming weight (number of nonzero elements) of the vector does not exceed the correcting ability of the algebraic block code used:

$$0 \le w(e) \le t = \left[\frac{d-1}{2}\right].$$

For each formed secret text $C_j \in C_{k-h_j}$, the corresponding vector $e = \left(e_0, e_1, \ldots, e_{n-1}\right)$ acts as a one-time session key, i.e. for a particular E_j the vector e is generated randomly equiprobably and independently of the other closed texts.

The communication channel receives $C_j^* = C_j - C_{k-h_j}$.

On the receiving side, an authorized user who knows the disguise rule, the number and location of zero information symbols can use a fast algebrogeometric code decoding algorithm (with polynomial complexity) to recover the plaintext [4]:

$$M_i = f_u^{-1}\left(C_j^*, \left\{X, P, D\right\}_u\right).$$

To recover the plaintext, an authorized user adds zero information symbols $C_j^* = C_j + C_{k-h_j}$, from the recovered secret text C_j, removes the effect of the secret permutation and diagonal matrices P^u and D^u :

$$\begin{aligned} C = C_j^* \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} = \left(M_i \times \left(G_X^u\right)^T + e\right) \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} = \\ = \left(M_i \times \left(X^u \times G \times P^u \times D^u\right)^T + e\right) \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} = \\ = M_i \times \left(X^u\right)^T \times \left(G\right)^T \times \left(P^u\right)^T \times \left(D^u\right)^T \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} + e \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} = \\ = M_i \times \left(X^u\right)^T \times \left(G\right)^T + e \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1}, \end{aligned}$$

decodes the received vector by the Berlekamp-Massey algorithm [26, 27]:

$$C = M_i \times \left(X^u\right)^T \times \left(G^{EC}\right)^T + e \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1},$$

i.e. gets rid of the second term and from the multiplier $\left(G\right)^{EC^T}$ in the first term in the right side of the equation, and then removes the effect of the disguise matrix X^u. For this, the result of decoding $M_i \times \left(X^u\right)^T$ should be multiplied by $\left(X^u\right)^{-1}$: $\left(M_i \times \left(X^u\right)^T\right) \times \left(X^u\right)^{-1} = M_i$. The resulting solution is the plain text M_i.

The block diagram of the real-time information exchange protocol using the asymmetric cryptosystem based on the modified McEliece CCC with modified (shortened) elliptic codes (*MEC*) is shown in **Fig. 4.7**.

Let us consider the practical algorithms of formation and decryption/decoding cryptogram/codegram in a modified asymmetric crypto-code system based on the McEliece CCC on elliptic shortened codes. **Fig. 4.8** shows an algorithm of cryptogram/codegram formation, in **Fig. 4.9** presents an algorithm for decoding information.

Mathematical model of modified asymmetric crypto-code information (MACCS) protection system using algebraic block codes based *on McEliece CCC* based on elongation (information symbols increasing) is formally defined by combination of the following elements:

– multiplicity of plaintexts $M = \left\{M_1, M_2, \ldots, M_{q^k}\right\}$, where $M_i = \left\{I_0, I_{h_{r1}}, \ldots I_{h_{rj}}, I_{k-1}\right\}$, $\forall I_j \in GF\left(q\right)$, h_j – information symbols equal to zero, $|h| = 1/2k$, i.e. I_i=0, $\forall I_i \in h$; h_r – information symbols of lengthening k, $|h| = 1/2k$;

– multiplicity of closed texts (*codegrams*) $C=\{C_1,C_2,\ldots,C_{q^k}\}$, where $C_i=\left(A^*_{X_0},A^*_{h_{r1}},\ldots,A^*_{h_{rj}},A^*_{X_{n-1}}\right)$, $\forall A^*_{X_j}\in GF(q)$;

– multiplicity of straight mappings (based on the use of generating matrix public key) $\varphi=\{\varphi_1,\varphi_2,\ldots,\varphi_s\}$, where $\varphi_i:M\to C_{h_r}$, $i=1,2,\ldots,s$;

– multiplicity of reverse mappings (based on the use of masking matrix private key) $\varphi^{-1}=\{\varphi_1^{-1},\varphi_2^{-1},\ldots,\varphi_s^{-1}\}$, where $\varphi_i^{-1}:C_{h_r}\to M$, $i=1,2,\ldots,s$;

– multiplicity of keys, parametrizing straight mapping (the public key of an authorized user) $K_{a_i}=\left\{K_{1_{a_i}},K_{2_{a_i}},\ldots,K_{s_{a_i}}\right\}=\left\{G^{EC_1}_{X_{a_i}},G^{EC_2}_{X_{a_i}},\ldots,G^{ECs}_{X_{a_i}}\right\}$, where $G^{EC_i}_{X_{a_i}}$ – generating $n\times k$ matrix masked as a random algebra-geometric block (*n*, *k*, *d*) code with elements from $GF(q)$, i.e. $\varphi_i:M\xrightarrow{K_{ia_i}}C_{hr}$, $i=1,2,\ldots,s$;

– a_i – multiplicity of coefficients of the polynomial curve $a_1\ldots a_6$, $\forall a_i\in GF(q)$, uniquely defining a specific set of curve points from the space P^2.

– multiplicity of keys, parameterizing reverse mappings (personal (private) key of authorized user) $K^*=\{K_1^*,K_2^*,\ldots,K_s^*\}=\left\{\{X,P,D\}_1,\{X,P,D\}_2,\ldots,\{X,P,D\}_s\right\}$, $\{X,P,D\}_\mathrm{i}=\{X^i,P^i,D^i\}$, where X^i – masking nondegenerate randomly equiprobably formed by source of keys matrix $k\times k$ with elements from $GF(q)$; P^i – permutational randomly equiprobably formed by source of keys matrix $n\times n$ with elements from $GF(q)$; D^i – diagonal formed by source of keys matrix $n\times n$ with elements from $GF(q)$, i.e. $\varphi_i^{-1}:C\xrightarrow{K_i^*}M$, $i=1,2,\ldots,s$.

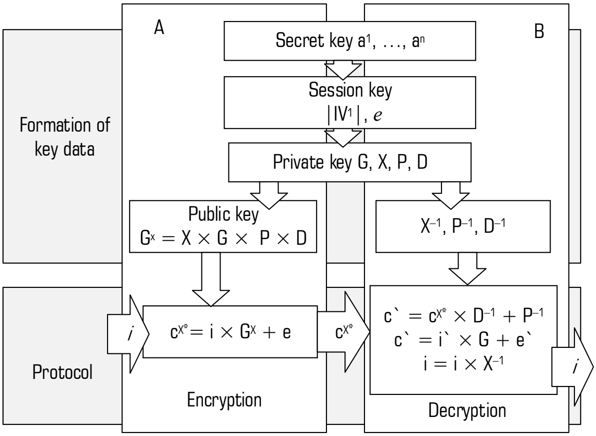
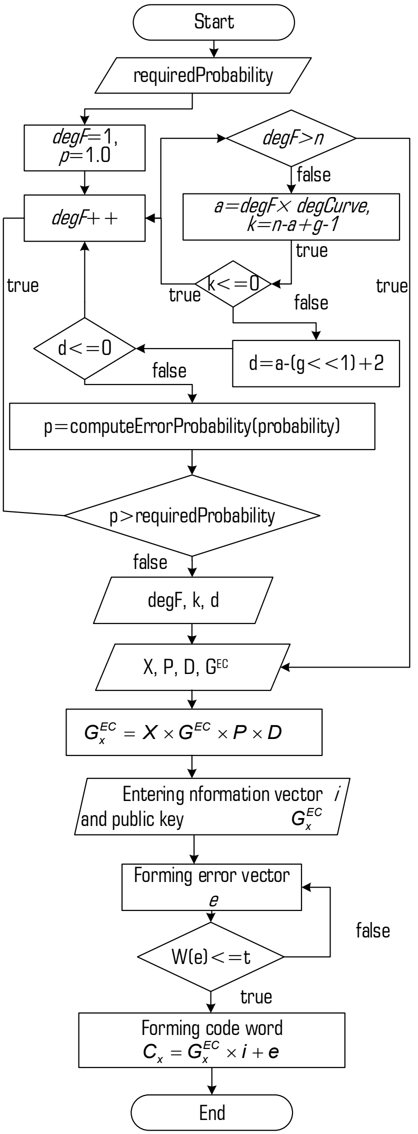


Fig. 4.7 Protocol using the asymmetric cryptosystem based on the modified McEliece CCC with modified (shortened) elliptic codes

Complexity of performing reverse mapping φ_i^{-1} without knowledge a key $K_i^*\in K^*$ associated with solution of theoretic complexity problems in random code decoding (generic position code).

Initial data in the description of the considered asymmetric crypto-code information protection systems are the parameters described in the previous model.



Stage 1. Set code parameters

requiredProbability – defined probability of block distortion;
n – total number of symbols in code (code length);
k – number of information symbols;
d – minimal distance of code combinations by Hemming;
g – curve genus;
degF – the degree of generating function;
degCurve – curve degree

Stage 2. Forming private and public keys of asymmetric cryptosystem, entering information package

X – non-degenerate matrix $k\times k$ over $GF(q)$;
P – permutational matrix $n\times n$ over $GF(q)$;
D – diagonal matrix $n\times n$ over $GF(q)$;
G^{EC} – check matrix $r\times n$ of elliptic code over $GF(q)$;
a^i – coefficients set of curve polynomial $a^1...a^6$

Stage 3. Forming session key and codegram

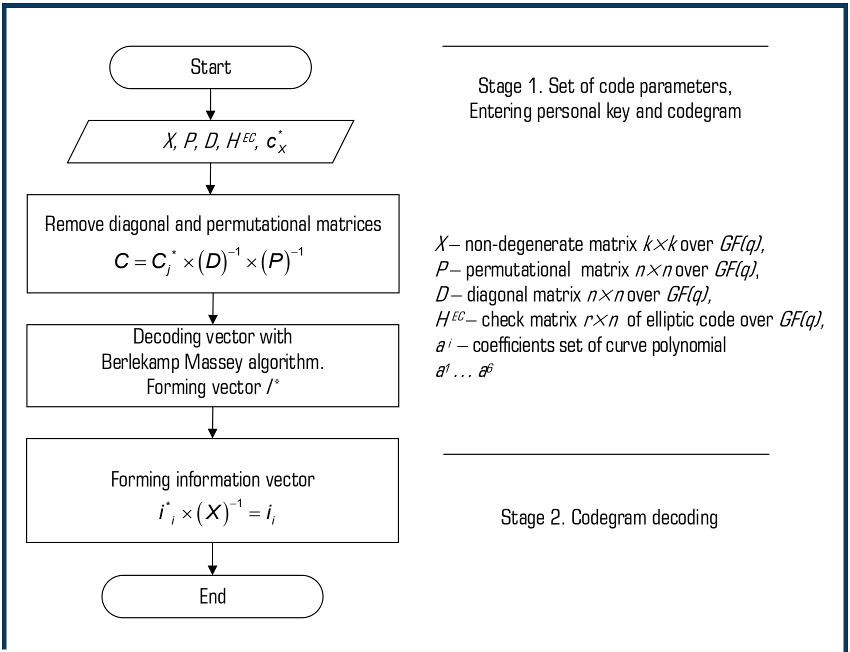
vector e forms randomly,equiprobably and independently from another secret texts; communication channel receives code without zero elements of initialization vector (shortening operation)

Fig. 4.8 The algorithm of codegram formation in the modified McEliece ACCS with shortened modified code

In asymmetric crypto-code system based on McEliece TCS modified (elongated) algebrogeometric (n, k, d) code C_{h_r} with rapid decoding algorithm is masking random (n, k, d) code $C^*_{h_r}$ by multiplying generating matrix G^{EC} of C_{k-h_j} code on the secret masking matrices X^u, P^u and D^u, what provide formation of open key for authorized user:

$$G_X^{EC_u} = X^u \times G^{EC} \times P^u \times D^u, u \in \{1,2\ldots,s\},$$

where G^{EC} – generating $n \times k$ matrix of algebrogeometric (n, k, d) code with elements from $GF(q)$, built on the basis of using the polynomial curve coefficients $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, chose by user, uniquely defining a specific set of curve points from the space P^2.


Start
X, P, D, H^{EC}, c^*_X
Remove diagonal and permutational matrices
$C = C_j^* \times (D)^{-1} \times (P)^{-1}$
Decoding vector with Berlekamp Massey algorithm. Forming vector I^*
Forming information vector
$i^*_i \times (X)^{-1} = i_i$
End
Stage 1. Set of code parameters, Entering personal key and codegram
X – non-degenerate matrix $k \times k$ over $GF(q)$,
P – permutational matrix $n \times n$ over $GF(q)$,
D – diagonal matrix $n \times n$ over $GF(q)$,
H^{EC} – check matrix $r \times n$ of elliptic code over $GF(q)$,
a^i – coefficients set of curve polynomial
$a^1 \ldots a^6$
Stage 2. Codegram decoding

⬡ **Fig. 4.9** Algorithm for decoding information in the modified McEliece CCC with shortened modified code

Forming secret text $C_j \in C_{h_r}$ by the entered plaintext $M_i \in M$ and given public key $G_{X_{a_i}}^{ECu}$, $u \in \{1,2\ldots,s\}$ is performed by forming of shortened code word and then elongation of masked code with adding to its randomly formed vector $e = (e_0, e_1, \ldots e_{n-1})$:

$$C_j = \varphi_u(M_i, G_X^u) = M_i \times (G_X^u)^T + e.$$

For each formed secret text $C_j \in C_{h_r}$ the appropriate vector $e = (e_0, e_1, \ldots e_{n-1})$ acts as a single session key, i.e. for specific E_j, vector e is formed randomly, equiprobably and independently of the other secret texts.

The channel receives $C_j^{\,*} = C_j - C_{k-h_j} + C_{h_r}$.

On the receiving side, an authorized user who knows the rule of masking, the number and location of zero information symbols can take advantage of a fast-decoding algorithm of algebro-geometric code (with polynomial complexity) to recover the plaintext:

$$M_i = f_u^{-1}\left(C_j^*, \{X,P,D\}_u\right).$$

To recover the plaintext an authorized user replaces lengthening symbols on non-zero information symbols:

$$C_j^* = C_{h_r} \rightarrow C_{k-h_j},$$

from recovered secret text C_j reduces the effect of the secret of permutational and diagonal matrices P^u and D^u:

$$\begin{aligned}
C &= C_j^* \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} = \left(M_i \times \left(G_X^{EC_u}\right)^T + e\right) \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} = \\
&= \left(M_i \times \left(X^u \times G^{EC} \times P^u \times D^u\right)^T + e\right) \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} = \\
&= M_i \times \left(X^u\right)^T \times \left(G^{EC}\right)^T \times \left(P^u\right)^T \times \left(D^u\right)^T + e \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} = \\
&= M_i \times \left(X^u\right)^T \times \left(G^{EC}\right)^T + e\left(D^u\right)^{-1} \times \left(P^u\right)^{-1},
\end{aligned}$$

decodes received vector with Berlekamp-Massey algorithm:

$$C = M_i \times \left(X^u\right)^T \times \left(G^{EC}\right)^T + e\left(D^u\right)^{-1} \times \left(P^u\right)^{-1},$$

i.e. get rid of the second term and from the multiplier $(G)^{ECT}$ in the first term at right side of equation, and then reduces the effect of masking matrix X^u.

Received result of decoding M^*_i is need to be multiplied by $\left(X^u\right)^{-1}$:

$$M_i^* \times \left(X^u\right)^{-1} = M_i.$$

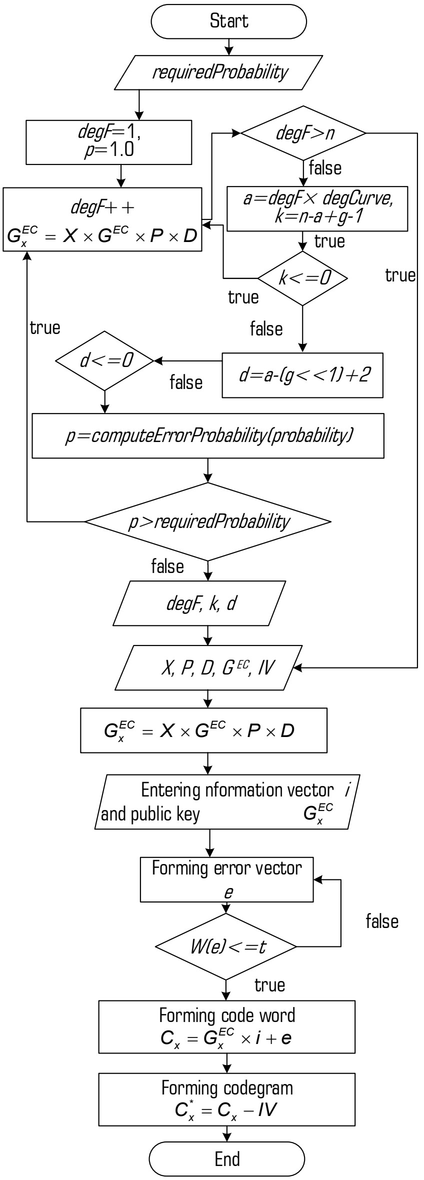
Received solution is plaintext M_i, to which are added lengthening symbols: $M_j = M_i + h_r$ – the essence of sent message.

Consider the practical algorithms of codegram forming and decoding, and a block diagram of communication protocol in a real time at developed McEliece CCC.

Fig. 4.10 shows algorithm of encoding in McEliece CCC.

Offered decoding algorithm on McEliece CCC is shown on **Fig. 4.11**.

Block diagram of information exchange protocol in a real time mode with the use of asymmetric cryptosystems based on a modified McEliece CCC with modified (elongated) elliptical codes is shown in **Fig. 4.12**.



Stage 1. Set code parameters

requiredProbability – defined probability of block distortion;
n – total number of symbols in code (code length);
k – number of information symbols;
d – minimal distance of code combinations by Hemming;
g – curve genus;
degF – the degree of generating function;
degCurve – curve degree.

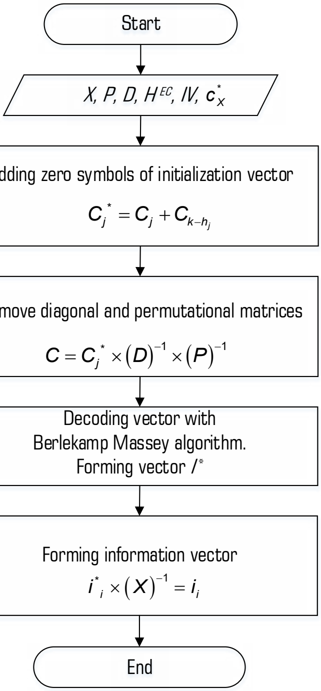
Stage 2. Forming private and public keys of asymmetric cryptosystem, entering information package

X – non-degenerate matrix *k*× *k* over *GF(q)*;
P – permutational matrix *n*× *n* over *GF(q)*;
D – diagonal matrix *n*× *n* over *GF(q);*
G^{EC} – check matrix *rxn* of elliptic code over *GF(q)*;
a^i – coefficients set of curve polynomial $a^1 \ldots a^6$;
IV – initialization vector,
IV=|h|=1/2k – reducing elements.

Stage 3. Forming session key and codegram

vector *e* forms randomly,equiprobably and independently from another secret texts; communication channel receives code without zero elements of initialization vector (shortening operation)

Fig. 4.10 Algorithm of codegram formation in McEliece MACCS


Start
$X, P, D, H^{EC}, IV, c_X^*$
Adding zero symbols of initialization vector
$C_j^* = C_j + C_{k-h_j}$
Remove diagonal and permutational matrices
$C = C_j^* \times (D)^{-1} \times (P)^{-1}$
Decoding vector with
Berlekamp Massey algorithm.
Forming vector I^*
Forming information vector
$i^*_i \times (X)^{-1} = i_i$
End

Stage 1. Set of code parameters,
Entering personal key and codegram

X – non-degenerate matrix $k \times k$ over $GF(q)$,
P – permutational matrix $n \times n$ over $GF(q)$,
D – diagonal matrix $n \times n$ over $GF(q)$,
H^{EC} – check matrix $r \times n$ of elliptic code over $GF(q)$,
a^i – coefficients set of curve polynomial
$a^1 \dots a^6$,
IV – initialization vector,
IV$= |h| = ½\,k$ – reducing elements

Stage 2. Codegram decoding

Fig. 4.11 Algorithm of codegram decoding in McEliece CCC

The *mathematical model of the modified asymmetric crypto-code system of information protection using algebraic geometric block codes based on CCC McEliece based on elongation (increase of information symbols) is formally defined* by a set of the following elements:

– set of plaintexts: $M = \{M_1, M_2, \dots, M_{q_k}\}$, where $M_i = \{I_0, I_{h_{r1}}, \dots I_{h_{rj}}, I_{k-1}\}$, $\forall I_j \in GF(q)$, h_j – information symbols equal to zero, $|h| = 1/2k$, that is $I_i = 0$, $\forall I_i \in h$; h_r – information extension symbols k, $|h| = 1/2k$;

– set of closed texts (*codograms*): $C = \{C_1, C_2, \dots, C_{q_k}\}$, where $C_i = \left(A^*_{X_0}, A^*_{h_{r1}}, \dots, A^*_{h_{rj}}, A^*_{X_{n-1}}\right)$, $\forall A^*_{X_j} \in GF(q)$;

– set of direct mappings (based on the use of the public key – the generating matrix): $\varphi = \{\varphi_1, \varphi_2, \dots, \varphi_s\}$, where $\varphi_i : M \to C_{h_r}$, $i = 1,2,\dots,s$;

– set of inverse mappings (based on the use of private (private) key – masking matrices): $\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \dots, \varphi_s^{-1}\}$, where $\varphi_i^{-1} : C_{h_r} \to M$, $i = 1,2,\dots,s$;

– a set of keys that parameterizes direct mappings (public key of an authorized user): $K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, \dots, K_{s_{a_i}}\} = \{G^{EC_1}_{X_{a_i}}, G^{EC_2}_{X_{a_i}}, \dots, G^{ECs}_{X_{a_i}}\}$, where $G^{EC_i}_{X_{a_i}}$ – generative $k \times n$ matrix of algebraic geometric block disguised as a random code (n, k, d) with elements from $GF(q)$, that is $\varphi_i : M \xrightarrow{K_{ia_i}} C_{hr}$, $i = 1,2,\dots,s$;

– a_i – set of coefficients of the polynomial curve $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, which uniquely defines a specific set of curve points from space P^2;

– a set of keys that parameterizes the inverse mappings (private (private) key of the authorized user):

$$K^* = \{K_1^*, K_2^*, \ldots, K_s^*\} = \{\{X,P,D\}_1, \{X,P,D\}_2, \ldots, \{X,P,D\}_s\},$$

$$\{X,P,D\}_i = \{X^i, P^i, D^i\},$$

where X^i – masking nondegenerate accidentally equally likely formed by the source of the keys $k \times k$ matrix with elements of $GF(q)$; P^i – permutative is randomly equally likely formed by the source of keys $n \times n$ matrix with elements of $GF(q)$; D^i – diagonal formed by the source of the keys $n \times n$ matrix with elements of $GF(q)$, that is $\varphi_i^{-1}: C \xrightarrow{K_i^*} M$, $i = 1,2,\ldots,s$, the difficulty of performing the inverse mapping φ_i^{-1} without knowledge of the key $K_i^* \in K^*$ associated with solving a theoretically complex problem – decoding a random code (general position code).

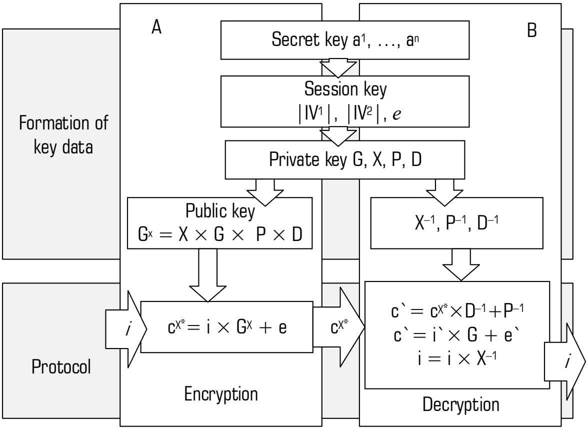


Fig. 4.12 Protocol in a real time mode with the use of asymmetric cryptosystems based on a modified McEliece CCC with modified (elongated) elliptical codes

The initial data in the description of the considered MNCCS are the parameters described in the previous model.

In McEliece CCC modified (extended) algebrogeometric (n, k, d) code C_{h_r} with a fast decoding algorithm disguised as random (n, k, d) code $C_{h_r}^*$ by multiplying the generating matrix G^{EC} of the code C_{k-h_j} by the masking matrix, which are kept secret X^u, P^u and D^u, which provides the formation of the public key of the authorized user:

$$G_X^{EC_u} = X^u \times G^{EC} \times P^u \times D^u, \quad u \in \{1,2,\ldots,s\},$$

where G^{EC} – generating matrix of algebraic geometric block (n, k, d) code with elements from $GF(q)$, is based on the use of user-selected coefficients of the polynomial of the curve $a_1 \dots a_6$, $\forall a_i \in GF(q)$, which uniquely defines a specific set of curve points from space P^2.

Formation of closed text $C_j \in C_{h_r}$ on the entered plaintext $M_i \in M$ and the specified public key $G^{ECu}_{X_{a_i}}$, $u \in \{1,2,\dots,s\}$ is carried out by forming a shortened codeword, and then extending the masked code with the addition of a randomly generated vector $e = (e_0, e_1, \dots, e_{n-1})$:

$$C_j = \varphi_u\left(M_i, G^u_X\right) = M_i \times \left(G^u_X\right)^T + e.$$

For each formatted closed text $C_j \in C_{h_r}$ corresponding vector $e = (e_0, e_1, \dots, e_{n-1})$ acts as a one-time session key, i.e. is formed randomly, equally probably and independently of other private texts.

In the communication channel enters:

$$C_j^* = C_j - C_{k-h_j} + C_{h_r}.$$

On the receiving side, an authorized user who knows the masking rule, the number and location of zero information symbols can use a fast algorithm for decoding algebraic geometric code (polynomial complexity) to recover plaintext:

$$M_i = \varphi_u^{-1}\left(C_j^{-1}, \{X,P,D\}_u\right).$$

To restore the plaintext, the authorized user replaces the extension symbols with zero information symbols:

$$C_j^{\,*} = C_{h_r} \to C_{k-h_j},$$

from the restored closed text removes the effect of secret permutation and diagonal matrices P^u and D^u:

$$\begin{aligned} C &= C_j^* \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} = \left(M_i \times \left(G^{EC_u}_X\right)^T + e\right) \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} = \\ &= \left(M_i \times \left(X^u \times G^{EC} \times P^u \times D^u\right)^T + e\right) \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} = \\ &= M_i \times \left(X^u\right)^T \times \left(G^{EC}\right)^T \times \left(P^u\right)^T \times \left(D^u\right)^T + e \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} = \\ &= M_i \times \left(X^u\right)^T \times \left(G^{EC}\right)^T + e\left(D^u\right)^{-1} \times \left(P^u\right)^{-1}, \end{aligned}$$

decodes the obtained vector according to the Berlekamp – Massey algorithm:

$$C = M_i \times \left(X^u\right)^T \times \left(G^{EC}\right)^T + e\left(D^u\right)^{-1} \times \left(P^u\right)^{-1},$$

that is, it gets rid of the second term and the multiplier $(G)^{ECT}$ in the first term in the right part of equality, then removes the effect of the masking matrix X^u.

For this purpose, the received decoding result M_i^* should be multiplied by $(X^u)^{-1}$:

$$M_i^* \times (X^u)^{-1} = M_i.$$

The resulting solution is plain text M_i, to which extension symbols are added: $M_j = M_i + h_r$ and is a transmitted message.

The main properties of MES are given in **Table 4.3**, the main parameters of MNCCS in **Table 4.4**. To construct a modified crypto-code Niederreiter system, we use basic algorithms of encryption/decryption of the system, discussed in [125].

Table 4.3 Basic (n, k, d) properties of *MEC*

Properties	Shorted *MEC*	Elongated *MEC*
(n, k, d) parameters of the code which is constructed through mapping of a kind φ: $X \to P^{k-1}$	$n = 2\sqrt{q} + q + 1 - x$, $k \geq \alpha - x$, $d \geq n - \alpha$, $\alpha = 3 \times degF$, $k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq \alpha - x + x_1$, $d \geq n - \alpha$, $\alpha = 3 \times degF$
(n, k, d) parameters of the code which is constructed through mapping of a kind φ: $X \to P^{r-1}$	$n = 2\sqrt{q} + q + 1 - x$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \times degF$, $k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \times degF$

Table 4.4 The main parameters of MNKKS McEliece at *MEC*

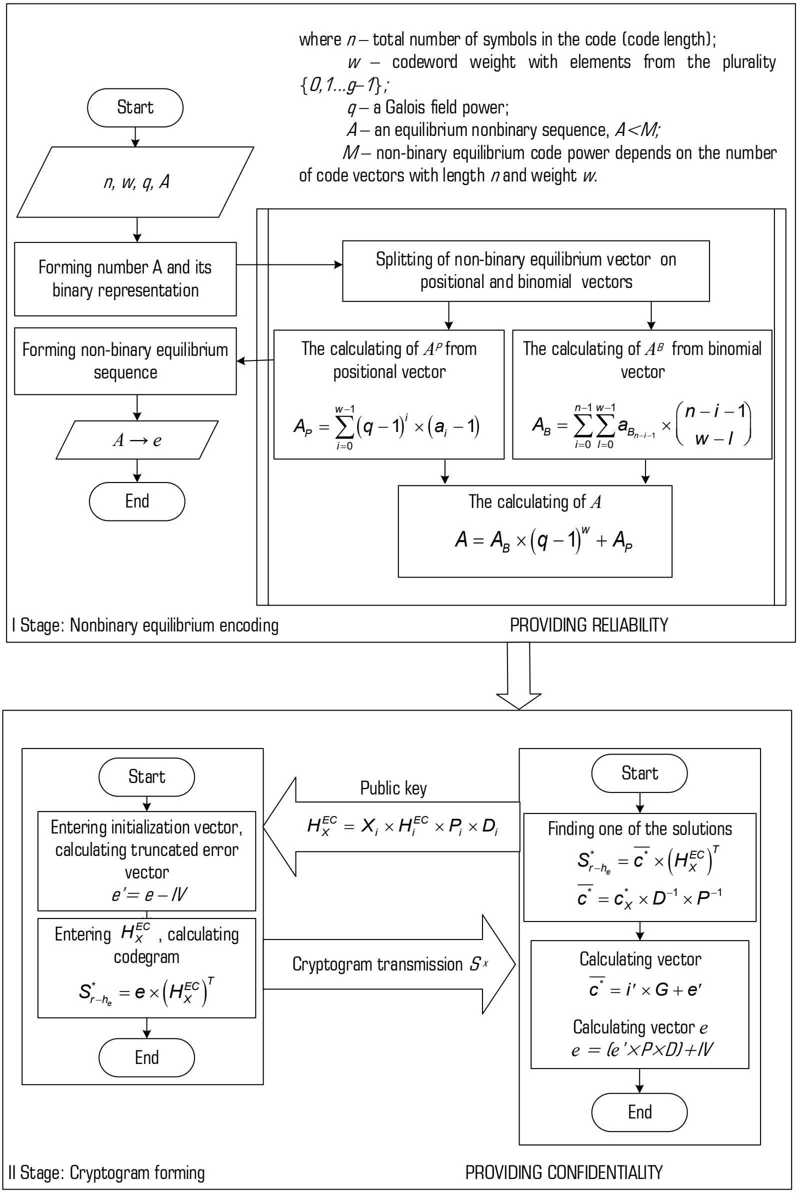
Properties	Shorted *MEC*	Elongated *MEC*
the dimension of the secret key	$l_{K+} = x \times \left[\log_2\left(2\sqrt{q} + q + 1\right)\right]$	$l_{K+} = (x - x_1) \times \log_2\left(2\sqrt{q} + q + 1\right)$
dimension of the information vector	$l_I = (\alpha - x) \times m$	$l_I = (\alpha - x + x_1) \times m$
dimension of the cryptogram	$l_S = \left(2\sqrt{q} + q + 1 - x\right) \times m$	$l_S = \left(2\sqrt{q} + q + 1 - x + x_1\right) \times m$
relative transmission rate	$R = (\alpha - x) / \left(2\sqrt{q} + q + 1 - x\right)$	$R = (\alpha - x + x_1) / \left(2\sqrt{q} + q + 1 - x + x_1\right)$

Fig. 4.13 shows a block diagram of the Niederreiter MCCS, the main difference of which from the known is the use of the mechanism of shortening the error vector symbols after the equilibrium coding algorithm, which will reduce the capacity of the used $GF(q)$ and energy capacity of the computing system in general.

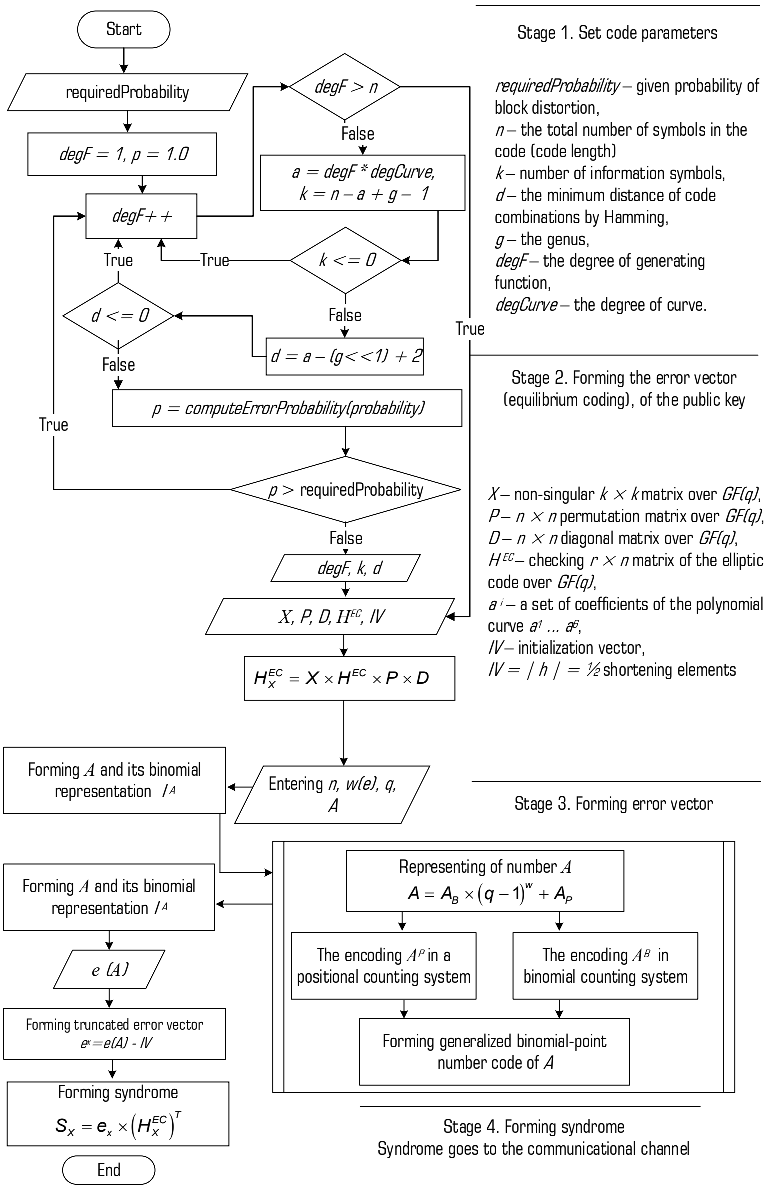
Algorithms for encryption and decryption are shown in **Fig. 4.14**, **4.15** accordingly.

Analysis of the practical implementation of code-converting algorithms in Niederreiter MCCS shows that when forming the codegram based on the initialization vector, shortening is performed – h_e (error vector symbols equal to zero), $|h| = 1/2e$, i.e. $e_i = 0$, $\forall e_i \in h$. When decryption of the cryptogram (after receiving the error vector, before using the equilibrium encryption algorithm) to obtain information «zero» shortening symbols are introduced.

Let us consider the formal description of a modified asymmetric crypto code Niederreiter system through the use of the modified elliptical codes.


where *n* – total number of symbols in the code (code length);
w – codeword weight with elements from the plurality $\{0,1...g-1\}$;
q – a Galois field power;
A – an equilibrium nonbinary sequence, $A<M$;
M – non-binary equilibrium code power depends on the number of code vectors with length *n* and weight *w*.
Start
n, w, q, A
Forming number A and its binary representation
Forming non-binary equilibrium sequence
$A \to e$
End
Splitting of non-binary equilibrium vector on positional and binomial vectors
The calculating of A^P from positional vector
$A_P = \sum_{i=0}^{w-1}(q-1)^i \times (a_i - 1)$
The calculating of A^B from binomial vector
$A_B = \sum_{i=0}^{n-1}\sum_{l=0}^{w-1} a_{B_{n-i-1}} \times \binom{n-i-1}{w-l}$
The calculating of *A*
$A = A_B \times (q-1)^w + A_P$
I Stage: Nonbinary equilibrium encoding
PROVIDING RELIABILITY
Start
Entering initialization vector, calculating truncated error vector
$e' = e - IV$
Entering H_X^{EC}, calculating codegram
$S^*_{r-h_e} = e \times (H_X^{EC})^T$
End
Public key
$H_X^{EC} = X_i \times H_i^{EC} \times P_i \times D_i$
Cryptogram transmission S^x
Start
Finding one of the solutions
$S^*_{r-h_e} = \overline{c^*} \times (H_X^{EC})^T$
$\overline{c^*} = c_X^* \times D^{-1} \times P^{-1}$
Calculating vector
$\overline{c^*} = i' \times G + e'$
Calculating vector *e*
$e = (e' \times P \times D) + IV$
End
II Stage: Cryptogram forming
PROVIDING CONFIDENTIALITY

⬡ **Fig. 4.13** Structural diagram of a modified Niederreiter CCC


Start
requiredProbability
degF = 1, p = 1.0
degF++
degF > n
False
a = degF * degCurve,
k = n – a + g – 1
True
True
k <= 0
d <= 0
False
False
d = a – (g<<1) + 2
p = computeErrorProbability(probability)
True
True
p > requiredProbability
False
degF, k, d
X, P, D, H^EC, IV
$H_X^{EC} = X \times H^{EC} \times P \times D$
Forming A and its binomial representation I^A
Entering n, w(e), q, A
Forming A and its binomial representation I^A
Representing of number A
$A = A_B \times (q-1)^w + A_P$
The encoding A^P in a positional counting system
The encoding A^B in binomial counting system
Forming generalized binomial-point number code of A
e (A)
Forming truncated error vector
e^x=e(A) - IV
Forming syndrome
$S_X = e_x \times \left(H_X^{EC}\right)^T$
End

Stage 1. Set code parameters

requiredProbability – given probability of block distortion,
n – the total number of symbols in the code (code length)
k – number of information symbols,
d – the minimum distance of code combinations by Hamming,
g – the genus,
degF – the degree of generating function,
degCurve – the degree of curve.

Stage 2. Forming the error vector (equilibrium coding), of the public key

X – non-singular $k \times k$ matrix over *GF(q)*,
P – $n \times n$ permutation matrix over *GF(q)*,
D – $n \times n$ diagonal matrix over *GF(q)*,
H^{EC} – checking $r \times n$ matrix of the elliptic code over *GF(q)*,
a^i – a set of coefficients of the polynomial curve $a^1 \dots a^6$,
IV – initialization vector,
$IV = | h | = ½$ shortening elements

Stage 3. Forming error vector

Stage 4. Forming syndrome
Syndrome goes to the communicational channel

Fig. 4.14 The algorithm for generating the cryptogram in the Niederreiter CCC

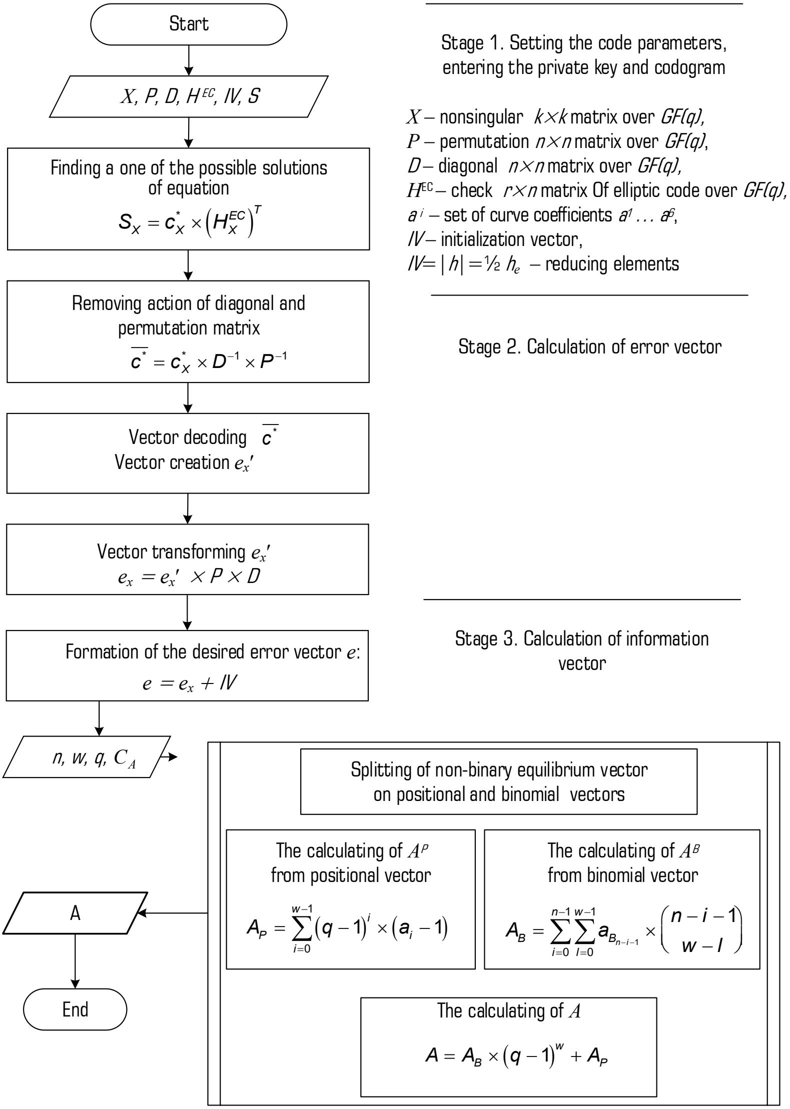

Start
X, P, D, H^{EC}, IV, S
Finding a one of the possible solutions of equation
$S_X = c_X^* \times \left(H_X^{EC}\right)^T$
Removing action of diagonal and permutation matrix
$\overline{c^*} = c_X^* \times D^{-1} \times P^{-1}$
Vector decoding $\overline{c^*}$
Vector creation e_x'
Vector transforming e_x'
$e_x = e_x' \times P \times D$
Formation of the desired error vector e:
$e = e_x + IV$
n, w, q, C_A
A
End
Stage 1. Setting the code parameters, entering the private key and codogram
X – nonsingular $k \times k$ matrix over $GF(q)$,
P – permutation $n \times n$ matrix over $GF(q)$,
D – diagonal $n \times n$ matrix over $GF(q)$,
H^{EC} – check $r \times n$ matrix Of elliptic code over $GF(q)$,
a^i – set of curve coefficients $a^1 \ldots a^6$,
IV – initialization vector,
$IV = |h| = ½\, h_e$ – reducing elements
Stage 2. Calculation of error vector
Stage 3. Calculation of information vector
Splitting of non-binary equilibrium vector on positional and binomial vectors
The calculating of A^P from positional vector
$A_P = \sum_{i=0}^{w-1} (q-1)^i \times (a_i - 1)$
The calculating of A^B from binomial vector
$A_B = \sum_{i=0}^{n-1} \sum_{l=0}^{w-1} a_{B_{n-i-1}} \times \binom{n-i-1}{w-l}$
The calculating of A
$A = A_B \times (q-1)^w + A_P$

Fig. 4.15 The algorithm for cryptogram decryption in the Niederreiter CCC

A mathematical model of the NCCS with using of the Niederreiter code-theoretic schemes (CTS) based on shortening (reducing of information symbols after converting in the error *vector in the algorithm of non-binary equilibrium coding)* is formally given by the combination of the following elements [125]:

– h_e – symbols of the error vector equal to zero, $|h| = 1/2e$, i. e $e_i = 0$, $\forall e_i \in h$;

– a set of private texts (*codegrams*) – $S = \left\{S_0, S_1, \ldots S_{q^r}\right\}$, where $S_i = \left\{S^*_{X_0}, S^*_{h_1}, \ldots S^*_{h_j}, S^*_{X_r}\right\}$, $\forall S_{X_r} \in GF(q)$;

– a set of keys, parametrizing direct mapping (the public key of an authorized user) $KU_{a_i} =$ $= \left\{KU_{1_{a_i}}, KU_{2_{a_i}}, \ldots, KU_{r_{a_i}}\right\} = \left\{H^{EC_1}_{X_{a_i}}, H^{EC2}_{X_{a_i}}, \ldots, H^{ECr}_{X_{a_i}}\right\}$, where $H^{EC_i}_{X_{a_i}}$ – check $r \times n$ matrix of algebrogeometric block (*n, k, d*) code, disguised as random code with elements from *GF*(*q*) i.e. $\varphi_i : M \xrightarrow{KU_{i_{a_i}}} S^*{}_{r-h_e}$, $i = 1,2,\ldots,e$.

Initial data in the description of the considered modified crypto-code information protection system are:

– algebra-geometric block (*n, k, d*)-code over *GF*(*q*);

– *w* – weight of codeword with elements from the set $\{0,1\ldots g-1\}$, *q* – power of the Galois field, *n* – error vector length; *A* – non-binary equilibrium sequence, $A<M$; *M* – power of non-binary equilibrium code defined by the number of vectors of length *n* and weight *w*;

– a_i – a set of coefficients of the polynomial of the curve $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, clearly defining a specific set of points on the curve in space P^2 to form generating matrix;

– *IV* – initializing vector, $IV = |h| = 1/2h_e$ – reducing elements (h_e – error vector symbols equal to zero, $|h| = 1/2e$, i.e. $e_i = 0$, $\forall e_i \in h$);

– disguising matrix mappings, given by a set of matrixes $\left\{X, P, D\right\}_i$, where *X* – nondegenerate $k \times k$ matrix over *GF*(*q*), *P* – permutation $n \times n$ matrix over *GF*(*q*) with one non-zero element in each line and each row of the matrix, *D* – diagonal $n \times n$ matrix over *GF*(*q*) with non-zero elements on the main diagonal.

In the modified Niederraiter crypto-code system on modified (truncated) algebra-geometric (*n, k, d*)-codes, the information vector is converted in fast algorithm of non-binary equilibrium coding into the error vector.

After the operation of shortening, the error vector is disguised as a random syndrome by multiplying the truncated error vector by the public key of the recipient (the check matrix H^{EC}_X of the code):

$$KU_{a_i} = H^{EC}_X = X^i \times H^{EC} \times P^i \times D^i, i \in \left\{1,2,\ldots,r\right\}.$$

Communication channel receives $S^*_{r-h_e} = \left(e_n - h_e\right) \times H^{ECT}_X$.

On the receiving side, an authorized user who knows the disguise rule, the initialization vector (the number and places of zero characters in the error vector) can use a fast algebra-geometric decoding algorithm (polynomial complexity) to recover the plaintext:

$$M_i = \varphi_i^{-1}\left(S^*_{r\text{-}h_e}, \left\{X, P, D\right\}_i\right).$$

To restore the plaintext, an authorized user searches for one of the solutions of equations:

$$S^*_{r-h_e} = \bar{c}^* \times \left(H^{EC}_X\right)^T.$$

«Undisguises» the codeword, obtained in the previous step $\overline{c}_x^* = \overline{c}^* \times D^{-1} \times P^{-1}$, decodes the obtained vector by the Berlekamp-Massey algorithm, forms the error vector according to the Chen procedure e'_x, transforms into the vector e'_x by multiplying the previous result of the error vector by disguising matrixes *P, D*:

$$e_X = e'_x \times P \times D.$$

Forming of the desired error vector *e* to convert into information vector based on a fast algorithm of non-binary equilibrium coding:

$$e = e_x + IV.$$

Transformation of the vector e based on the use of non-binary equilibrium code into the information sequence. Thus, modified Niederreiter crypto-code system is presented, which allows to reduce the energy capacity of the group operations by shortening symbols in the error vector (reducing the syndrome symbols and power of the used Galois field), to increase the entropy of characters of closed texts, transmitted to the communication channel and thus provide the required cryptographic resistance.

4.5 HYBRID ASYMMETRIC CRYPTO-CODE CONSTRUCTIONS OF MCELIECE AND NIEDERREITER BASED ON DEFECTIVE CODES

In articles [148, 149], authors considered theoretical and practical fundamentals for the construction of flawed codes. A flawed text is understood to be a text obtained by further deformation of the non-redundant letter codes.

Thus, the necessary and sufficient condition for the flawed text with its meaning lost is a reduction in the lengths of text character codes outside of their redundancy. Consequently, a flawed text is of length that is less than the length of the original text, and it has no meaning of the original text [148].

Theoretical basis for constructing flawed texts is the removal of the orderliness of the original text characters and, consequently, a reduction in the redundancy of language symbols in the flawed text. In this case, amount of information indicating this orderliness will be equal to a reduction in entropy of the text as compared to the maximally possible magnitude of entropy, that is, equiprobable appearance of any letter after any previous letter.

Text redundancy will be calculated from formula:

$$B(M) = B_A L_0 = \left(\log N - \frac{H(M)}{L_0}\right) \times L_0,$$

where *M* is the original text; *B* is the language redundancy ($B = R - r$, *R* is the absolute entropy of a language, $R = \log N$, *N* is the alphabet power, *r* is the entropy of language per one character,

$r = H(M)/L$, L is the length of message M in language characters); $H(M)$ is the entropy (uncertainty) of the message; L_0 is the length of message M in language characters with a meaning; B_A is the language redundancy.

In order to obtain a flawed text (*FTC*) and a damage (*DCH*), a «perfect» compression method is used after performing m cycles of damaging mechanism C_m [148, 149].

The number of cycles required to minimize the length of the original text is equal to:

$$m > \frac{\log n - B_A}{\log \eta},$$

where n is the representation power of the original text character; B_A is the language redundancy; η is the number of times the length of the original text in *MV*2 is reduced in each step (a certain constant coefficient).

A quantitative measure of the effectiveness of damage is the degree of destruction of the meaning, equal to the difference in entropies of the flawed text and the original text in different intervals of length of the flawed text:

$$d = H(FTC) - \sum_{i=1}^{s} H(M_i)p_i, \quad \sum_{i=1}^{s} p_i = 1,\ s = \left[\frac{L_0 - L_{FTC}}{L_{FTC}}\right],$$

where M_i is part of the original text, corresponding to the i-th interval, p_i is its probability, L_0 is the length M_i equal to length of L_{FTC} of the flawed text, s is the number of intervals. For an ergodic source of characters for the original text:

$$d_{\max} = \log L_{FTC} - H(M_i).$$

Fig. 4.16 shows a block diagram of one step of the universal damaging mechanism.

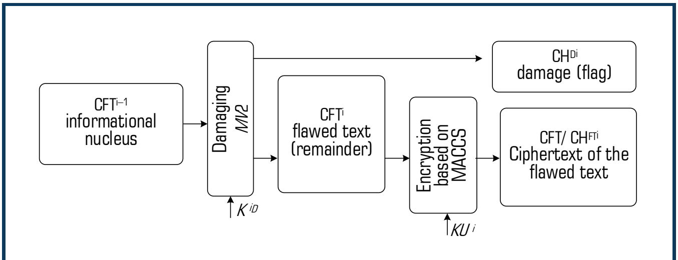

CFT^{i–1} informational nucleus
Damaging MV2
CFT^{i} flawed text (remainder)
Encryption based on MACCS
CH^{Di} damage (flag)
CFT/ CH^{FTi} Ciphertext of the flawed text
K^{iD}
KU^{i}

Fig. 4.16 Block diagram of one step of the universal mechanism for causing damage

In articles [28, 29], a *cyclic algorithm for obtaining the flawed texts* refers to the universal mechanism of causing damage (C_m, where m is the number of cycles), which implies a random replacement of the bit representation of each character of the original text with a tuple of a smaller or equal number of bits with their subsequent concatenation. **Fig. 4.17** shows a universal mechanism of causing damage (algorithm *MV*2 (formation of a flawed text)).

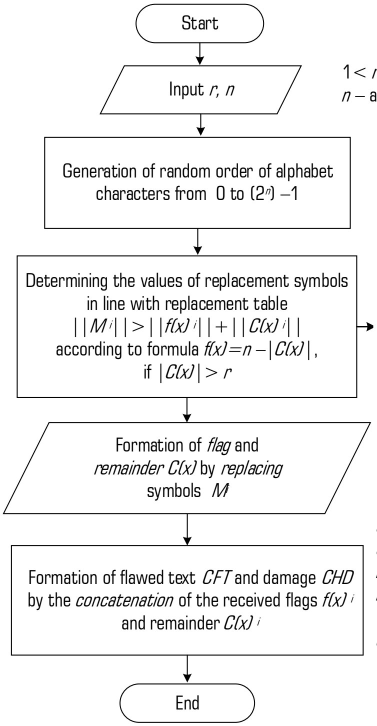
Domain of transformation determination in the *MV*2 algorithm – the set $\{0, 1\}^n$ – is considered to be the alphabet power of certain family of original texts, which are associated with a certain probability distribution of the letters of the given alphabet, while the characters of the original text are the value of a discrete random element.

Let X be a random discrete element that takes values $x_i \in \{0,1\}^n$ with probabilities p_i and $T = (c, f) \in F_n^r$ is the arbitrary fixed transformation *MV*2. Then for any $y \in U_{r\,n-1}$ (a certain binary line from a set of variable-length strings) and for any $1 \le i \le |y|$, the following holds:

$$\#\left\{x \in \{0,1\}^n : c(x) = y\right\} = \#\left\{x \in \{0,1\}^n : c(x) = y^{(i)}\right\}.$$

Then, regardless of the probability distribution of random element X, for the entropies of random elements FTC/FT_{CH} (flawed ciphertext) and CHD (damage), the following equalities hold:

$$H\left(FTC / FT_{CH}\right) \le \log\left(2^n - 2^r\right), \quad H\left(CHD\right) \le \log\left(n - r + 1\right).$$


Start
Input r, n
Generation of random order of alphabet characters from 0 to $(2^n) - 1$
Determining the values of replacement symbols in line with replacement table
$||M^i|| > ||f(x)^i|| + ||C(x)^i||$
according to formula $f(x) = n - |C(x)|$,
if $|C(x)| > r$
Formation of *flag* and *remainder C(x)* by *replacing* symbols M^i
Formation of flawed text *CFT* and damage *CHD* by the *concatenation* of the received flags $f(x)^i$ and remainder $C(x)^i$
End

$1 < r < n$ – positive integer
n – alphabet power

Symbol	Length of remainder	Remainder $C(x)$	Flag $f(x)$
S_1	r	0^r	$0^{n-r-1}1$
S_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
S_{2^r+1}	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$S_{2^{n-1}-2^r}$	$n-2$	1^{n-2}	01
$S_{2^{n-1}-2^r+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$S_{2^n-2^r}$	$n-1$	1^{n-1}	1
$S_{2^n-2^r+1}$	r	0^r	0^{n-r}
…	…	…	…
S_{2^n}	r	1^r	0^{n-r}

CFT/ CH^{FT} – ciphertext of flawed text
CHD/CH^{D} – ciphertext of damage
FTC/ FT^{CH} – damaged ciphertext
DCH/D^{CH} – damage to ciphertext
f(x) – flag (damage)
C(x) – remainder (flawed code)

Fig. 4.17 Universal mechanism for causing damage (algorithm *MV*2)

Thus, under uniform distribution of inputs (flags) of the algorithm *MV*2, a uniform distribution of the output (remainder) forms:

$$P\left(c_k = 0 \middle| 0 \le k \le \left|FTC / FT_{CH}\right\|\right) = \frac{1}{2}.$$

An analysis that we performed on the techniques of causing damage revealed that in order to use in IES, the most appropriate one is the first technique – causing damage with subsequent crypto-transformation, which makes it possible to reduce the alphabet power in the formation of a cryptogram in the McEliece MCCS. The distance of singularity for the given method (expression 1) will be transformed to:

$$U_0 = \frac{\sum_{i=1}^{m}\left(H\left(CHD^{(i)}\right)\right) + H(KU_i^{EC})}{B\log\left|I\right|}.$$

Such a system is based on the permanent distortion of damage and ensuring stability due to the subsequent use of the encryption based on MCCS. This leads to the impossibility to learn the ciphertext of the flawed text.

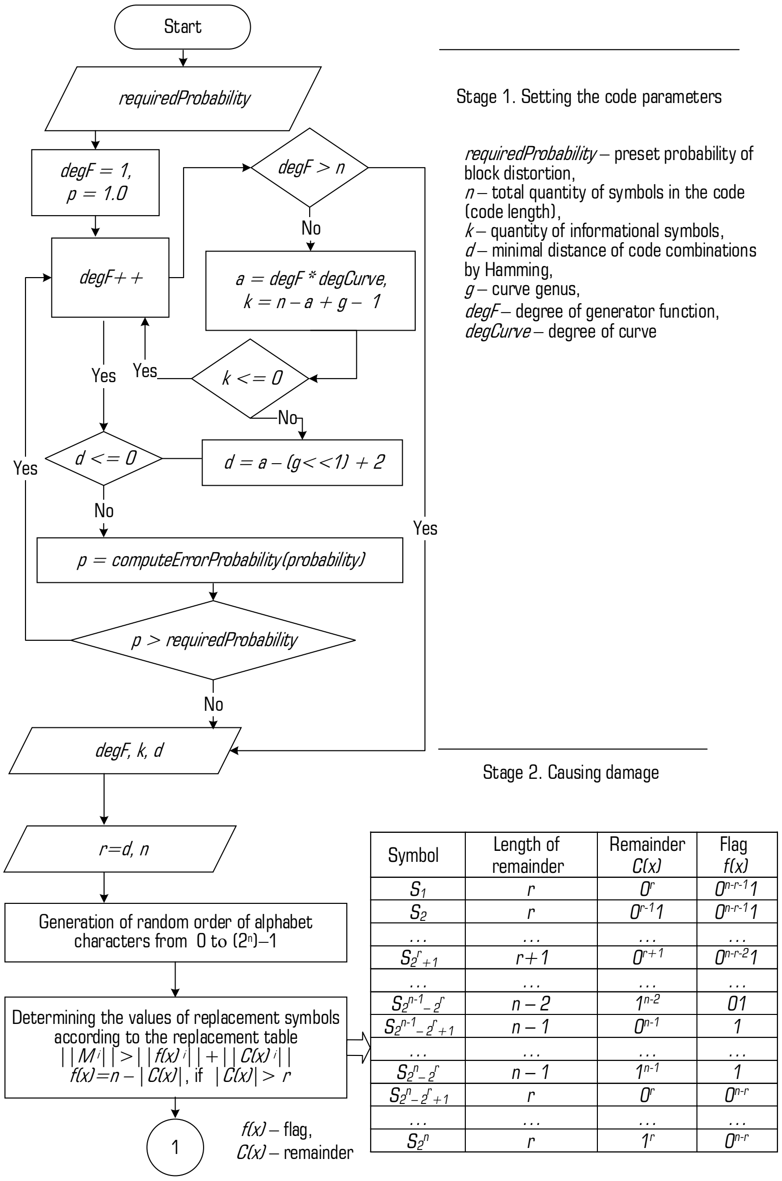
Thus, the analysis we performed of the basic principles for the construction of the McEliece MCCS and the multichannel cryptography systems on flawed codes allows us to design hybrid cryptosystems based on the modified asymmetric McEliece crypto-code systems and multichannel cryptography systems on flawed codes. A distinctive difference from the «classical» approach to the formation of a hybrid cryptosystem is the exploitation of asymmetric crypto-code constructions (that relate to secret models with provable stability) with fast crypto-transformations (a rate of transformation is comparable to the crypto-transformations in block-symmetric cipher (BSC) as a key mechanism for ensuring stability (safety) of information with subsequent application of the algorithm *MV*2 (a system on flawed codes) in order to reduce energy consumption (alphabet power of the McEliece MACCS) with the subsequent transmission along one or several channels. We shall consider practical algorithms for the formation of a cryptogram and decryption in the proposed hybrid cryptosystem.

Fig. 4.18, **4.19** show the algorithm for the formation of a cryptogram/codegram in a hybrid cryptosystem.

If the original text had a certain meaning, then, for such a system, flawed texts when using a brute force method over the entire field of encryption keys and key of damage have the only meaningful text equivalent to the original, provided that the length of the ciphertext exceeds the distance of singularity [149]. **Fig. 4.20** shows the decryption/decoding algorithm of a cryptogram in the proposed hybrid cryptosystem.

The algorithms proposed for the hybrid cryptosystem make it possible, when hiding the flawed ciphertext *CFT/CH*$_{FT}$, to improve entropy of the public key:

$$U_0 = \frac{H\left(CFT / CH_{FT}\right) + \sum_{i=1}^{m}\left(H\left(CHD^{(i)}\right)\right) + H\left(KU_i^{EC}\right)}{B\log\left|I\right|}.$$


Start
requiredProbability
degF = 1,
p = 1.0
degF > n
No
degF++
a = degF * degCurve,
k = n – a + g – 1
Yes
Yes
k <= 0
No
d <= 0
d = a – (g<<1) + 2
Yes
No
Yes
p = computeErrorProbability(probability)
p > requiredProbability
No
degF, k, d
r=d, n
Generation of random order of alphabet characters from 0 to (2ⁿ)–1
Determining the values of replacement symbols according to the replacement table
||Mⁱ|| > ||f(x)ⁱ|| + ||C(x)ⁱ||
f(x)=n – |C(x)|, if |C(x)| > r
1
f(x) – flag,
C(x) – remainder
Stage 1. Setting the code parameters
requiredProbability – preset probability of block distortion,
n – total quantity of symbols in the code (code length),
k – quantity of informational symbols,
d – minimal distance of code combinations by Hamming,
g – curve genus,
degF – degree of generator function,
degCurve – degree of curve
Stage 2. Causing damage

Symbol	Length of remainder	Remainder $C(x)$	Flag $f(x)$
S_1	r	0^r	$0^{n-r-1}1$
S_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
S_{2^r+1}	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$S_{2^{n-1}-2^r}$	$n-2$	1^{n-2}	01
$S_{2^{n-1}-2^r+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$S_{2^n-2^r}$	$n-1$	1^{n-1}	1
$S_{2^n-2^r+1}$	r	0^r	0^{n-r}
…	…	…	…
S_{2^n}	r	1^r	0^{n-r}

Fig. 4.18 Stages 1, 2 of the formation of a cryptogram in a hybrid cryptosystem based on the McEliece MACCS with flawed codes

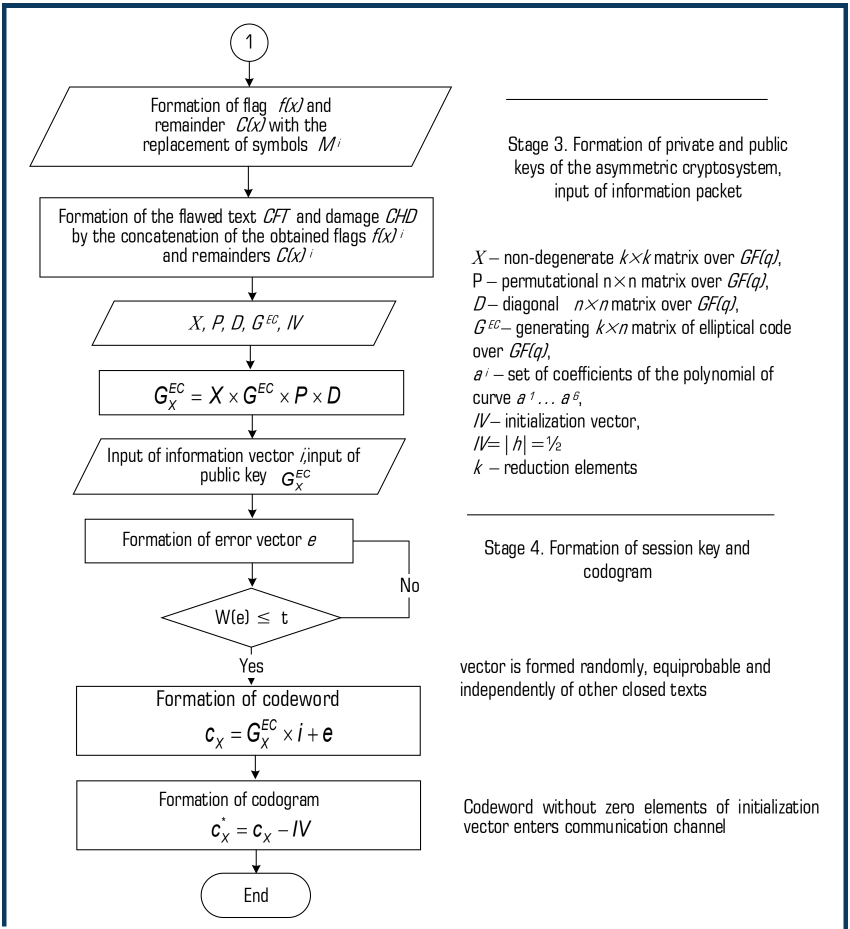
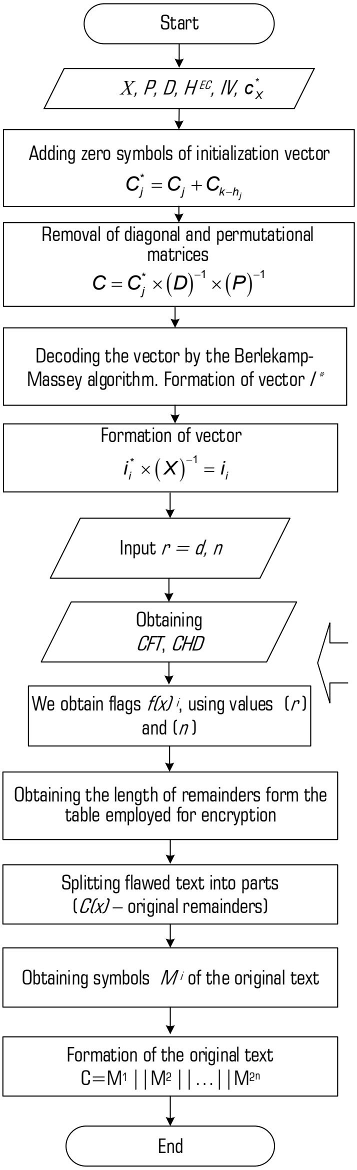

1
Formation of flag f(x) and remainder C(x) with the replacement of symbols M^i
Formation of the flawed text CFT and damage CHD by the concatenation of the obtained flags f(x)^i and remainders C(x)^i
X, P, D, G^EC, IV
$G_X^{EC} = X \times G^{EC} \times P \times D$
Input of information vector i,input of public key G_X^{EC}
Formation of error vector e
W(e) ≤ t
No
Yes
Formation of codeword $c_X = G_X^{EC} \times i + e$
Formation of codogram $c_X^* = c_X - IV$
End
Stage 3. Formation of private and public keys of the asymmetric cryptosystem, input of information packet
X – non-degenerate k×k matrix over GF(q),
P – permutational n×n matrix over GF(q),
D – diagonal n×n matrix over GF(q),
G^EC – generating k×n matrix of elliptical code over GF(q),
a^i – set of coefficients of the polynomial of curve a^1 ... a^6,
IV – initialization vector,
IV = |h| = ½
k – reduction elements
Stage 4. Formation of session key and codogram
vector is formed randomly, equiprobable and independently of other closed texts
Codeword without zero elements of initialization vector enters communication channel

Fig. 4.19 Stages 3, 4 of the formation of a cryptogram in a hybrid cryptosystem based on the McEliece MACCS with flawed codes

In the case of additional hiding of the last ciphertext of damage CHD/CH_D due to its smallness and proportionality with the flawed text ciphertext CFT/CH_{FT}, the distance of singularity can be further extended:

$$U_0 = \frac{H\left(CHD/CH_D\right) + H\left(CFT/CH_{FT}\right) + \sum_{i=1}^{m}\left(H\left(CHD^{(i)}\right)\right) + H\left(KU_i^{EC}\right)}{B\log\left|I\right|}.$$

Thus, a multichannel cryptography based on flawed codes makes it possible to integrate cryptographic systems, combining within the framework of one concept the crypto-code constructions (the McEliece MACCS) and the systems on flawed codes (*FC*), which, by complementing each other, will ensure the required safety and reliability parameters, as well as enrich the resulting system with their properties.


Start
$X, P, D, H^{EC}, IV, c^{*}_{X}$
Adding zero symbols of initialization vector
$C^{*}_{j} = C_{j} + C_{k-h_j}$
Removal of diagonal and permutational matrices
$C = C^{*}_{j} \times (D)^{-1} \times (P)^{-1}$
Decoding the vector by the Berlekamp-Massey algorithm. Formation of vector I^{*}
Formation of vector
$i^{*}_{i} \times (X)^{-1} = i_{i}$
Input $r = d, n$
Obtaining
CFT, CHD
We obtain flags $f(x)^{i}$, using values (r) and (n)
Obtaining the length of remainders form the table employed for encryption
Splitting flawed text into parts ($C(x)$ – original remainders)
Obtaining symbols M^{i} of the original text
Formation of the original text
$C=M^{1}||M^{2}||\ldots||M^{2n}$
End

Stage 1. Setting the parameters of code, input of private key and codogram

Stage 2. Decoding a codogram

Symbol	Length of the remainder	Remainder $C(x)$	Flag $f(x)$
M_1	r	0^{r}	$0^{n-r-1}1$
M_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
$M_{2^{r}+1}$	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$M_{2^{n-1}-2^{r}}$	$n-2$	1^{n-2}	01
$M_{2^{n-1}-2^{r}+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$M_{2^{n}-2^{r}}$	$n-1$	1^{n-1}	1
$M_{2^{n}-2^{r}+1}$	r	0^{r}	0^{n-r}
…	…	…	…
$M_{2^{n}}$	r	1^{r}	0^{n-r}

Stage 3. Restoring the message that was damaged

n – total quantity of symbols in the code (code length),
d – minimal distance of code combinations by Hamming,
$f(x)$ – flag,
$C(x)$ – remainder

Fig. 4.20 Decryption in a hybrid cryptosystem based on the McEliece MACCS

Cryptographic flawed texts are texts obtained in the following ways [142, 143]:

– *Approach 1*: damage to the source text with subsequent encryption of the defective text and/or its damage (**Fig. 4.21**);

– *Approach 2*: damage to the ciphertext (**Fig. 4.22**);

– *Approach 3*: damage to the source text and the ciphertext of the defective text (**Fig. 4.23**).

Thus, using the approach to damage the ciphertext with the Niederreiter's MCCC on the MEC, presented in **Fig. 4.23** (third approach) increases throughput starting from the *GF* field (2^9). This method is the best approach for building the Niederreiter hybrid MCCC for MEC. The synthesis of Niederreiter's MEC crypto-code construction with a cryptosystem on flawed codes proposed by the authors allows building complex (hybrid) crypto-code structures whose stability is determined by the strength of two cryptosystems to ensure the implementation of fast crypto-transformations by reducing the field power.

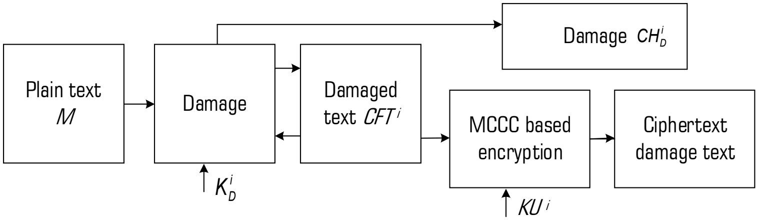


Fig. 4.21 Block diagram of building a hybrid cryptosystem based on damage to the source text (Approach 1)

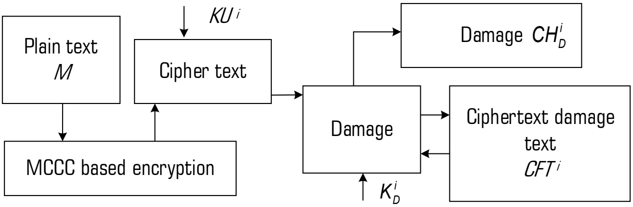


Fig. 4.22 Block diagram of the construction of a hybrid cryptosystem based on damage to the ciphertext (Approach 2)

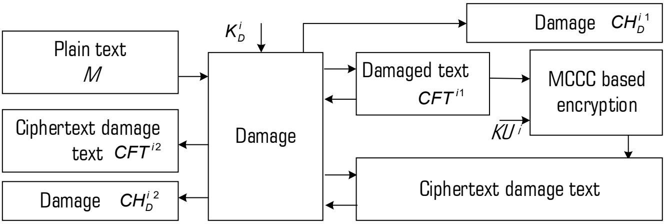


Fig. 4.23 Block diagram of building a hybrid cryptosystem based on damage to the source text and ciphertext (Approach 3)

Consider the algorithms for the practical implementation of the formation of a cryptogram and decoding based on the crypto-code design of the Niederreiter for MEC using defective texts and damaging the ciphertext. The encryption and decryption algorithms are shown in **Fig. 4.24**, **4.25** (encryption), **4.26**, **4.27** (decryption).

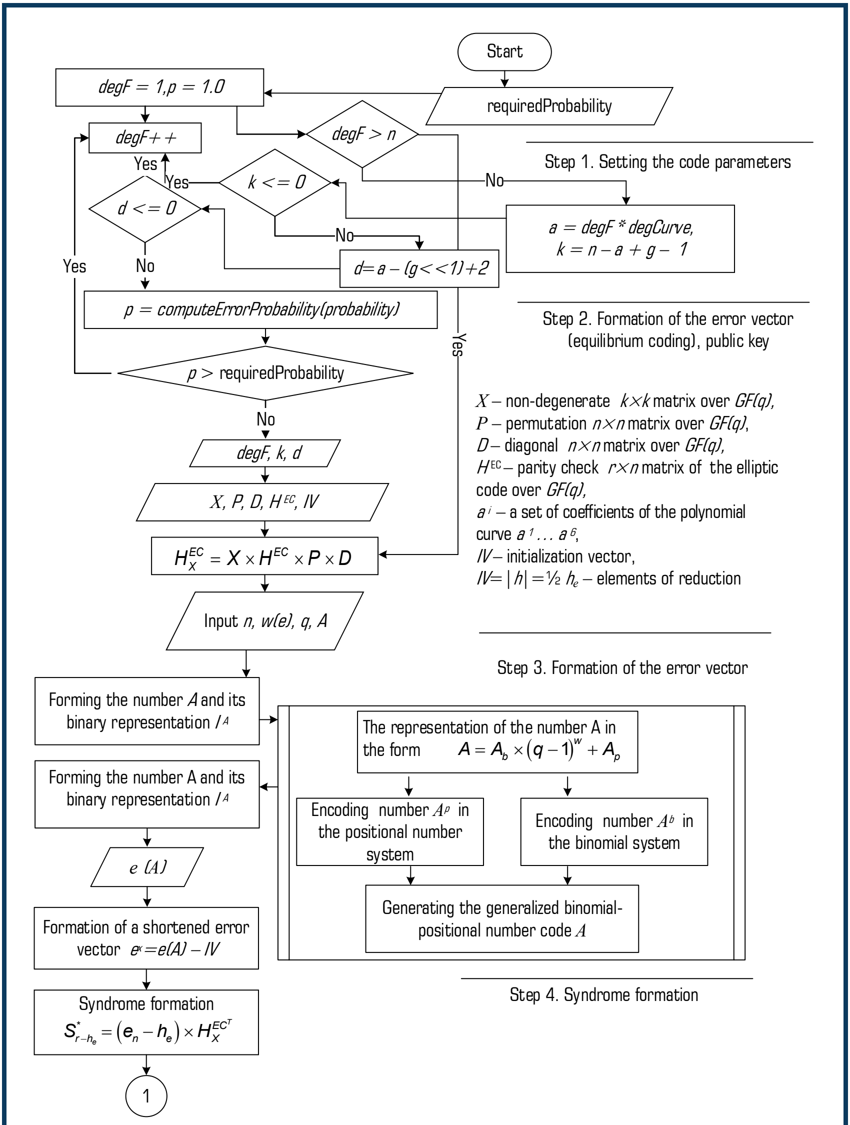
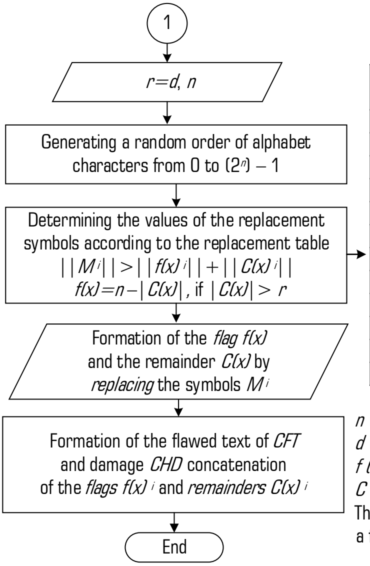

Start
requiredProbability
degF = 1,p = 1.0
degF > n
degF++
Yes
Yes
k <= 0
d <= 0
No
No
Step 1. Setting the code parameters
a = degF * degCurve,
k = n – a + g – 1
d=a – (g<<1)+2
Yes
No
p = computeErrorProbability(probability)
Step 2. Formation of the error vector (equilibrium coding), public key
Yes
p > requiredProbability
No
degF, k, d
X, P, D, H^EC, IV
$H_X^{EC} = X \times H^{EC} \times P \times D$
Input n, w(e), q, A
X – non-degenerate k×k matrix over GF(q),
P – permutation n×n matrix over GF(q),
D – diagonal n×n matrix over GF(q),
H^EC – parity check r×n matrix of the elliptic code over GF(q),
a^i – a set of coefficients of the polynomial curve a^1 ... a^6,
IV – initialization vector,
IV= | h| =½ h_e – elements of reduction
Step 3. Formation of the error vector
Forming the number A and its binary representation I^A
Forming the number A and its binary representation I^A
The representation of the number A in the form $A = A_b \times (q-1)^w + A_p$
Encoding number A^p in the positional number system
Encoding number A^b in the binomial system
Generating the generalized binomial-positional number code A
e (A)
Formation of a shortened error vector e^x=e(A) – IV
Step 4. Syndrome formation
Syndrome formation
$S^*_{r-h_e} = (e_n - h_e) \times H_X^{EC^T}$
1

Fig. 4.24 Algorithm for the formation of a cryptogram in the Niederreiter hybrid crypto-code system on flawed codes (HCCSFC)

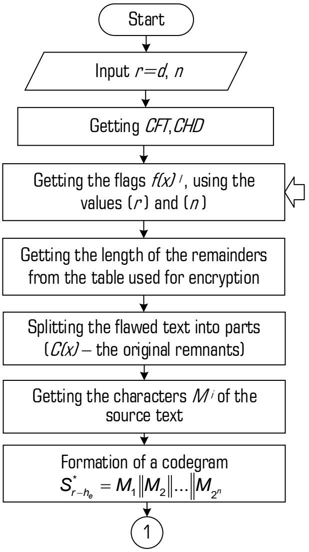

1
r=d, n
Generating a random order of alphabet characters from 0 to (2ⁿ) – 1
Determining the values of the replacement symbols according to the replacement table
| | M^i | | > | | f(x)^i | | + | | C(x)^i | |
f(x)=n–| C(x)|, if | C(x)| > r
Formation of the flag f(x) and the remainder C(x) by replacing the symbols M^i
Formation of the flawed text of CFT and damage CHD concatenation of the flags f(x)^i and remainders C(x)^i
End

Step 5. Damage

Symbol	Length of the remainder	Remainder $C(x)$	Flag $f(x)$
S_1	r	0^r	$0^{n-r-1}1$
S_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
S_{2^r+1}	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$S_{2^{n-1}-2^r}$	$n-2$	1^{n-2}	01
$S_{2^{n-1}-2^r+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$S_{2^n-2^r}$	$n-1$	1^{n-1}	1
$S_{2^n-2^r+1}$	r	0^r	0^{n-r}
…	…	…	…
S_{2^n}	r	1^r	0^{n-r}

n is the total number of characters in the code (code length),
d is the minimum distance of the Hamming code combinations,
f (x) is the flag,
C (x) is the remainder.
The channel / channels of communication receive
a flawed text (remainder) and damage (flag)

Fig. 4.25 Algorithm for the formation of a cryptogram in the Niederreiter HCCSFC


Start
Input r=d, n
Getting CFT, CHD
Getting the flags f(x)^i, using the values (r) and (n)
Getting the length of the remainders from the table used for encryption
Splitting the flawed text into parts (C(x) – the original remnants)
Getting the characters M^i of the source text
Formation of a codegram
$S^*_{r-h_e}=M_1\|M_2\|\ldots\|M_{2^n}$
1

Step 1. The formation of a meaningful codegram

Symbol	Length of the remainder	Remainder $C(x)$	Flag $f(x)$
M_1	r	0^r	$0^{n-r-1}1$
M_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
M_{2^r+1}	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$M_{2^{n-1}-2^r}$	$n-2$	1^{n-2}	01
$M_{2^{n-1}-2^r+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$M_{2^n-2^r}$	$n-1$	1^{n-1}	1
$M_{2^n-2^r+1}$	r	0^r	0^{n-r}
…	…	…	…
M_{2^n}	r	1^r	0^{n-r}

n is the total number of characters in the code (code length),
d is the minimum distance of the Hamming code combinations,
f (x) is the flag,
C (x) is the remainder

Fig. 4.26 Algorithm for decoding the cryptogram in the Niederreiter HCCSFC

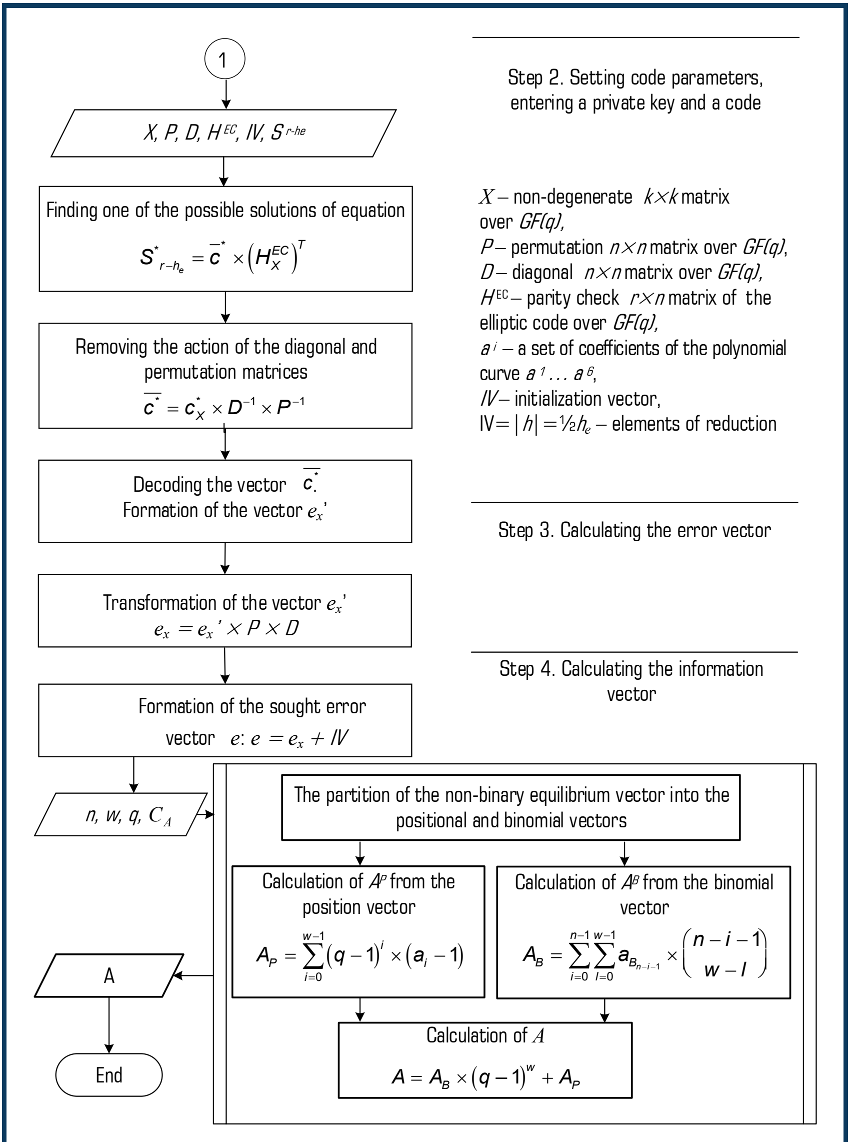

1
$X, P, D, H^{EC}, IV, S^{r\text{-}he}$
Finding one of the possible solutions of equation
$S^*_{r-h_e} = \bar{c}^* \times (H^{EC}_X)^T$
Removing the action of the diagonal and permutation matrices
$\bar{c}^* = c^*_X \times D^{-1} \times P^{-1}$
Decoding the vector $\bar{c}^*$.
Formation of the vector e_x'
Transformation of the vector e_x'
$e_x = e_x' \times P \times D$
Formation of the sought error vector e: $e = e_x + IV$
n, w, q, C_A
The partition of the non-binary equilibrium vector into the positional and binomial vectors
Calculation of A^P from the position vector
$A_P = \sum_{i=0}^{w-1} (q-1)^i \times (a_i - 1)$
Calculation of A^B from the binomial vector
$A_B = \sum_{i=0}^{n-1} \sum_{l=0}^{w-1} a_{B_{n-i-1}} \times \binom{n-i-1}{w-l}$
Calculation of A
$A = A_B \times (q-1)^w + A_P$
A
End
Step 2. Setting code parameters, entering a private key and a code
X – non-degenerate $k \times k$ matrix over $GF(q)$,
P – permutation $n \times n$ matrix over $GF(q)$,
D – diagonal $n \times n$ matrix over $GF(q)$,
H^{EC} – parity check $r \times n$ matrix of the elliptic code over $GF(q)$,
a^i – a set of coefficients of the polynomial curve $a^1 \ldots a^6$,
IV – initialization vector,
IV= $|h| = ½h_e$ – elements of reduction
Step 3. Calculating the error vector
Step 4. Calculating the information vector

Fig. 4.27 Algorithm for decoding the cryptogram in the Niederreiter HCCSFC

To determine the optimal method, we analyze the ratio of the number of required additional operations to implement the approach to the size of the resulting outgoing data. The dependence of group operations implementation ACCS from the power field is given in **Table 4.5**, in **Table 4.6** shows the length of the transmitted data, in **Table 4.7** – the ratio of these values shows the coefficient of bit throughput for each additional operation.

Table 4.5 Dependence of software implementation on field power (number of thousands of additional operations before encryption/after/amount)

Approach	2^5	2^7	2^9	2^{11}
1	1002/–/1002	3285/–/3285	6322/–/6322	11078/–/8247
2	–/1501/1501	–/4289/4289	–/9296/9296	–/15908/15908
3	992/1487/2479	2952/4428/7380	5793/8690/14483	10086/15130/25216

Table 4.6 The length of the transmitted data in bytes

Approach	2^5	2^7	2^9	2^{11}
1	500902	902403	1642357	2374489
2	375298	667029	1072313	1652979
3	627533	1044069	1868102	2716713

Table 4.7 Number of bits per additional operation

Approach	2^5	2^7	2^9	2^{11}
1	2.5E-04	4.55E-04	4.812E-04	4.341E-04
2	4.999E-04	8.038E-04	**10.836E-04**	**12.03E-04**
3	4.938E-04	8.836E-04	9.691E-04	11.602E-04

4.6 CONSTRUCTION OF METHODS OF STRICT AUTHENTICATION ON THE BASIS OF CRYPTO-CODE CONSTRUCTIONS OF MCELIECE AND NIEDERREITER

Two-factor authentication or 2FA is a user identification method in a service where two different types of authentication data are used. The introduction of an additional level of security provides better protection for your account against unauthorized access. Using this type of 2FA, the user enters personal password at the first authentication level. The next step, he must enter the OTP token (*OTP – One-time Password Algorithm*), usually sent via SMS to his mobile device. The OTP will be available only to those who, as supposed in theory, entered a password, inaccessible to unauthorized persons [125, 134, 135]. General classification of multi-factor authentication methods is shown in **Fig. 4.28** [135].

The analysis [134, 135, 150–152] of multifactor authentication methods showed the following main advantages and disadvantages:

– The advantages of the *methods based on SMS notification* are generation of the OTP code every time you log in and transmission through an additional channel, interception of the user's login and password in the main channel will not lead an attacker to client banking information. Binding of the OTP password to the customer's phone number. The main disadvantages are that the use of mobile open channel does not allow to ensure the confidentiality of the OTP code, using only cellular channels leads to a «loss» of two-factor authentication. There is a theoretical possibility of substitution of numbers the help of an operator or employees of mobile phone shops.

– The use of methods with applications-authenticators (QR Codes) allows you to have multiple accounts in a single authenticator and generate a primary key, there is no need to use ~~a~~ cellular communication lines, the generation of OTP passwords based on the cryptographic algorithms. The main disadvantages are the use of an authenticator on the device of entrance leads to the «loss» of two-factor authentication, an attacker access to the primary key of the user leads to the authentication system cracking.

– *Checking login via a mobile application* allows you to automate the authentication process without user interaction, based on verification of the personal authentication key on the mobile application. The main disadvantages are: the loss/disclosure of the private key results in the authentication system cracking, the possibility of receiving SMS messages by synchronization between the iPhone and the Mac, the use of the authenticator on the device~~,~~ of entrance leads to the «loss» of comprehensiveness.

– *The physical* (*or hardware*) *tokens* are the most reliable method of two-factor authentication. Most often, they are presented in the form of a USB stick with its own processor, generating cryptographic keys, which are automatically entered when you connect to a computer. The advantages are the absence of the need to use of additional mobile applications, software, tokens are completely independent devices. Disadvantages include multiple accounts lead to «binding» of tokens, not supported by all applications.

– *Backup keys* are the fall-back option in case of loss/theft of the smartphone, which receives one-time passwords or verification codes. Loss/theft of the backup key leads to the destruction of sensitive authentication system.

– *Barcodes of Passwindow system* provide unique static images of the sequence of symbols generated dynamically by the authentication server without the use of cryptographic algorithms. Any interference or tampering with the bar code is passively presented to the user in the form of combinations in a template that do not match the expectations. A significant disadvantage is the possibility of selecting a unique card barcode, proposed in [135].

– Using of *biometrics* as a secondary identification factor is performed by identifying the physical characteristics of a person (fingerprint, iris, etc.). The advantages of the methods include the use of a person's unique physiological characteristics, the absence of additional mobile applications and software. A significant disadvantage is the specific requirements for software and hardware devices of reading the user's biometric data.

Thus, multi-factor authentication systems based on one-time e-mail- or SMS-passwords and different types of tokens are generally used in automated banking systems. To ensure confidentiality of OTP codes, transmitted by the bank, in the remote banking standard, it is necessary to use the encrypted and operator-independent channel of their delivery. This approach is not affected by the majority of known threats, except for social engineering, exploiting the human factor.

Fig. 4.29 shows a synergetic approach to the classification of multi-factor authentication threats. The synergetic model [125] of threats to banking information provides necessary and sufficient conditions for the development of a new methodology aimed at achieving synergies in the field of security of public and private banking protection systems.

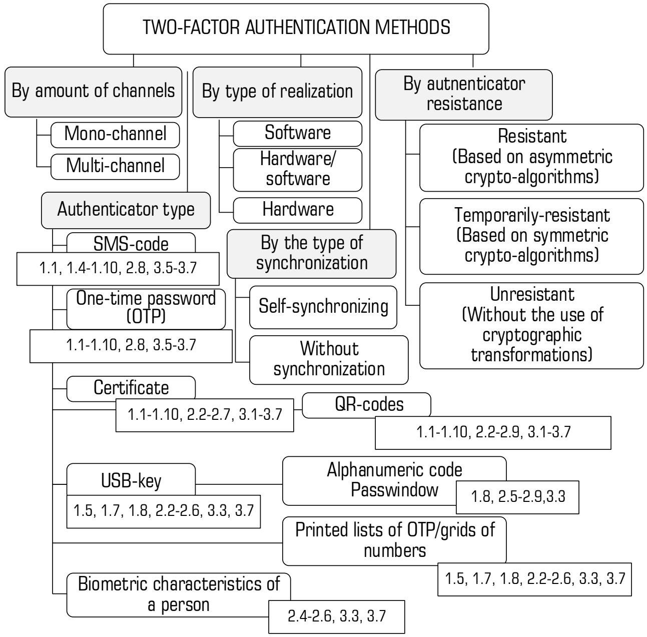


Fig. 4.28 Classification of multi-factor authentication methods

Thus, there is a need for additional means to ensure the confidentiality of information transmission in cellular communication systems.

Identification of *SMS systems* or multi-factor authentication systems based on mobile phones is wrong, a more precise term is an «out-of-band» authentication. However, with the spread of GSM, smartphones and tablets connected to the network, even this security advantage can be lost if the user transaction authentication is performed on the mobile device. In addition, the growth of unwanted software for mobile devices now allows an attacker to gain access to authentication codes sent via SMS not only through the traditional interception with the help of malicious software. Experts explain their decision by the fact that the SMS security faces new challenges with the introduction of VoIP services. Some of these services allow to hack the SMS system. NIST recommends developers to validate the use of VoIP connections before applying the SMS-based two-factor system. SMS protocol is considered unsafe [129]. The analysis of Internet attacks on multi-factor authentication schemes with SMS messages and advantages of crypto-code systems make it possible to improve the–multi-factor authentication scheme to enhance reliability and validity of the generated authenticator.

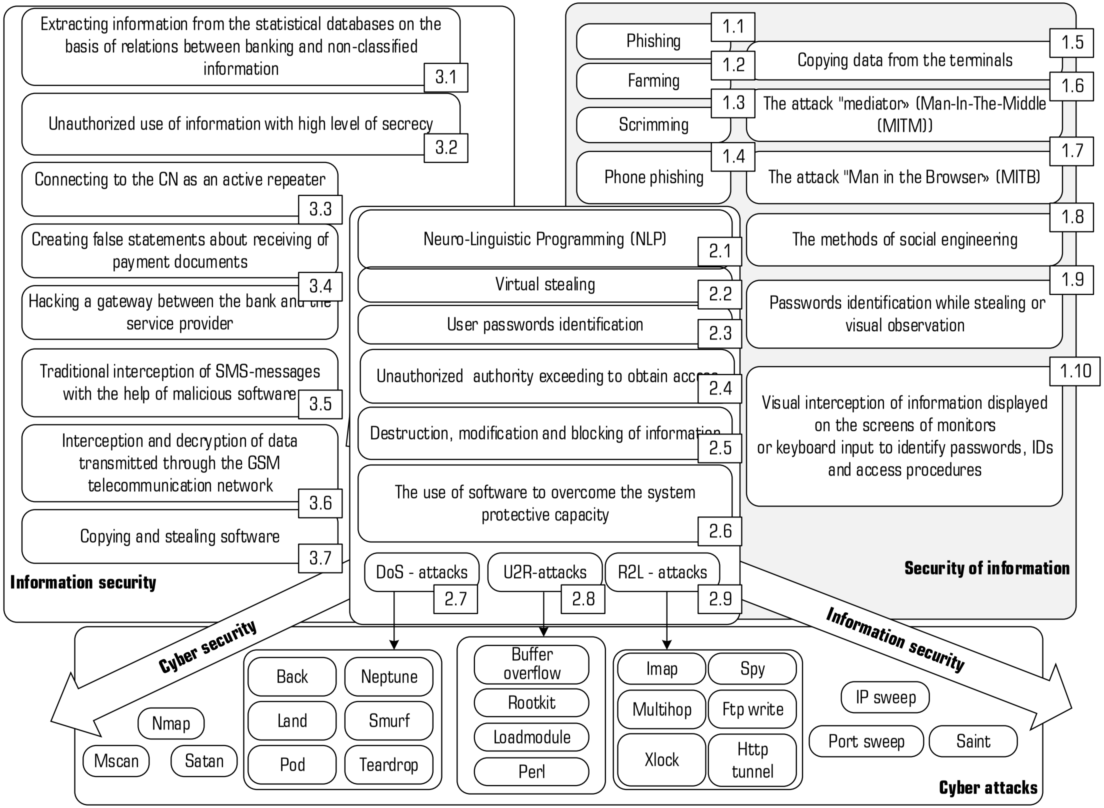

Extracting information from the statistical databases on the basis of relations between banking and non-classified information
3.1
Unauthorized use of information with high level of secrecy
3.2
Connecting to the CN as an active repeater
3.3
Creating false statements about receiving of payment documents
3.4
Hacking a gateway between the bank and the service provider
Traditional interception of SMS-messages with the help of malicious software
3.5
Interception and decryption of data transmitted through the GSM telecommunication network
3.6
Copying and stealing software
3.7
Information security
Phishing
1.1
Farming
1.2
Scrimming
1.3
Phone phishing
1.4
Copying data from the terminals
1.5
The attack "mediator» (Man-In-The-Middle (MITM))
1.6
The attack "Man in the Browser» (MITB)
1.7
The methods of social engineering
1.8
Passwords identification while stealing or visual observation
1.9
Visual interception of information displayed on the screens of monitors or keyboard input to identify passwords, IDs and access procedures
1.10
Security of information
Neuro-Linguistic Programming (NLP)
2.1
Virtual stealing
2.2
User passwords identification
2.3
Unauthorized authority exceeding to obtain access
2.4
Destruction, modification and blocking of information
2.5
The use of software to overcome the system protective capacity
2.6
DoS - attacks
2.7
U2R-attacks
2.8
R2L - attacks
2.9
Cyber security
Information security
Nmap
Mscan
Satan
Back
Neptune
Land
Smurf
Pod
Teardrop
Buffer overflow
Rootkit
Loadmodule
Perl
Imap
Spy
Multihop
Ftp write
Xlock
Http tunnel
IP sweep
Port sweep
Saint
Cyber attacks

Fig. 4.29 Synergetic model of banking information security threats

For this, a bank card (BC) must keep the following data elements [134]:

1. Certification authority public key index – since a terminal can work with multiple CAs, this value specifies which of the keys should be used by the terminal when working the given card.
2. Issuer public key certificate signed by the appropriate certification authority.
3. BC public key certificate is signed by the issuer and is based on the McEliece MCCS.
4. Issuer public key modulus and exponent.
5. BC public key modulus and exponent.
6. Banking card private key.

The terminal, that supports the multi-factor authentication scheme, must keep the public keys of all CAs and associated information relating to each of the keys.

The terminal must also be able to select the appropriate keys on the basis of the index (1) and some special identification information.

To support multifactor authentication, user banking card (BC) should have a personal key pair (public and private authenticator keys). The BC public key is stored on BC in its public key certificate. Each BC public key is certified by its issuer, and a trusted certification authority certifies the issuer public key. This means that to verify the authenticator card, the terminal must first verify two certificates in order to restore and authenticate the BC public key, which is then used for the BC authenticator verification.

The process of the proposed authentication consists of four stages:

– stage 1. Restoring the certificate authority public key by the terminal. The terminal reads the index (1), identifies and retrieves the certificate authority public key modulus – disguising matrix (*X, P, D*)*, curve equations for algebrogeometric code* (*AGC*), and associated information, stored in it,-selects the necessary algorithms;

– stage 2. Obtaining an initialization vector (secret «places» in the error vector – shortening bits) from the issuing bank. Forming the OTP code (error vector based on the Niederreiter modified crypto-code constraction (MCCC));

– stage 3. Forming an authenticator on the basis of using the McEliece MCCS. Obtaining a codeword (an authenticator) based on the use of the crypto-code system by adding the received codeword with a session key;

– stage 4. Finding the multiplicity of the error vector and the comparison with the obtained one. The structure of the proposed method of two-factor authentication based on the Niederreiter – McEliece MCCC is shown in **Fig. 4.30**.

In the authors' opinion, the significant advantage of using this multifactor authentication scheme is providing of required cryptographic resistance and reliability indexes of transmitted transactions with the use of Niederreiter – McEliece modified asymmetric crypto-code systems. The proposed mechanisms to ensure privacy: the transfer of SMS messages via cellular mobile communication channels with the Niederreiter MCCC (ensures the privacy of the OTP code) and the use of the McEliece MCCC in ABS digital channels (provides the OTP password transmission accuracy and confidentiality) would physically separate channels used for generating the banking transaction authenticator.

Using the session key at each transaction, the physical separation of the authenticator data transmission channels, scalability of the software module by changing the Niederreiter – McEliece

MCCC parameters, depending on the error rate in the used ABS communication channels will allow physical separation of transmission of the OTP-code of composite authenticator by the use of the two MCCC schemes in different communication channels and the required level of the 2FA protocol security in electronic banking applications.

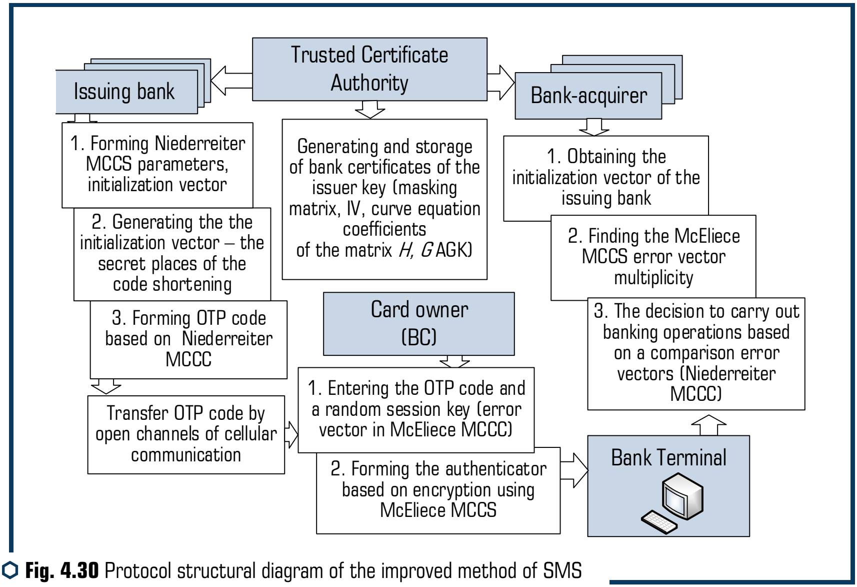

Trusted Certificate Authority
Issuing bank
Bank-acquirer
1. Forming Niederreiter MCCS parameters, initialization vector
2. Generating the the initialization vector – the secret places of the code shortening
3. Forming OTP code based on Niederreiter MCCC
Transfer OTP code by open channels of cellular communication
Generating and storage of bank certificates of the issuer key (masking matrix, IV, curve equation coefficients of the matrix H, G AGK)
Card owner (BC)
1. Entering the OTP code and a random session key (error vector in McEliece MCCC)
2. Forming the authenticator based on encryption using McEliece MCCS
1. Obtaining the initialization vector of the issuing bank
2. Finding the McEliece MCCS error vector multiplicity
3. The decision to carry out banking operations based on a comparison error vectors (Niederreiter MCCC)
Bank Terminal

Fig. 4.30 Protocol structural diagram of the improved method of SMS authentication based on the Niederreiter – McEliece MCCC

The proposed advanced method of strict two-factor authentication with OTP passwords based on McEliece and Niederreiter crypto-code systems allows eliminating the main disadvantage of the protocol 2FA – the transfer of individual authentication tokens via open mobile communication channels. For this purpose, crypto-code systems on flawed codes providing the required safety indices on the basis of encryption using the Niederreiter/McEliece asymmetric crypto-code system, the rate of crypto-transformations at the level of block cryptographic algorithms and the provision of data transmission with direct error correction have been proposed. This approach can be implemented in modern mobile and desktop applications using the protocols of GI and/or mobile networks.

A *schematic block diagram of practical implementation* of the proposed hybrid CCS (HCCS) on flawed codes is shown in **Fig. 4.31**.

Assessment of the cryptographic strength of the proposed HCCS on flawed codes.

To assess the cryptographic strength, we use the entropy method proposed in [122].

The proposed hybrid cryptosystem is comparable in stability with the second method of damage – damage to the ciphertext considered in [143, 144]. In this case, we have a set of flawed ciphertexts and damages, all individually not corresponding to the original meaningful text. With a complete set of flawed ciphertexts and all damages, the unicity distance increases due to additional keys of damage to the ciphertext. Thus, additional encryption provides an increased unicity distance:

$$U_0 = \left(\begin{array}{l} H\left(H^{EC}\right) + H\left(X_N^{EC}\right) + H\left(P_N\right) + H\left(D_N\right) + H\left(G^{EC}\right) + H\left(X_{Mc}^{EC}\right) + H\left(P_{Mc}\right) + \\ + H\left(D_{Mc}\right) + \sum_{i=1}^{m} H\left(\left(K^i_{MV2_N}\right) + H\left(K_i\right)\right) + \sum_{i=1}^{m} H\left(\left(K^i_{MV2_{Mc}}\right) + H\left(K_i\right)\right) \end{array} \right) \Bigg/ B \log\left|I\right|, \quad (4.4)$$

where U_0 is the unicity distance, H^{EC}, X_N^{EC}, P_N, D_N is the private key in the Niederreiter MCCS, G^{EC}, X_{Mc}^{EC}, P_{Mc}, D_{Mc} is the private key in the McEliece MCCS, $K^i_{MV2_N}$ is the key in the Niederreiter HCCS on flawed codes, $K^i_{MV2_{Mc}}$ is the key in the McEliece HCCS on flawed codes, $|I|$ is the number of meaningful texts, B is the number of texts, m is the number of damages.

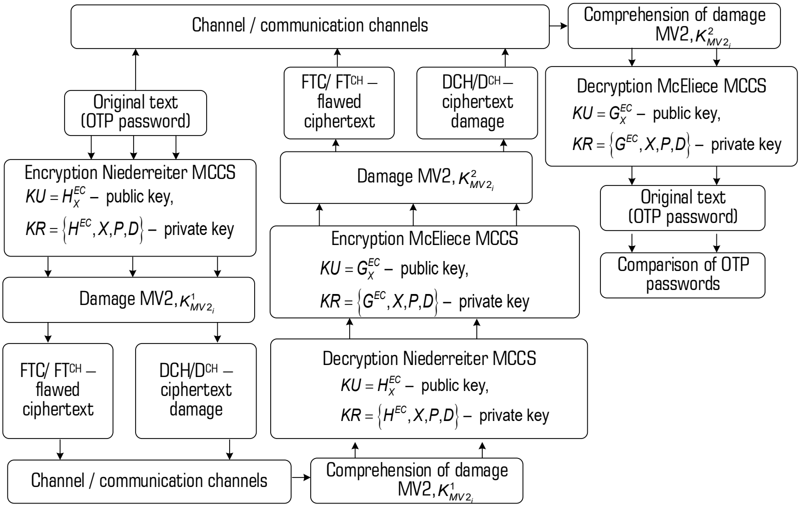
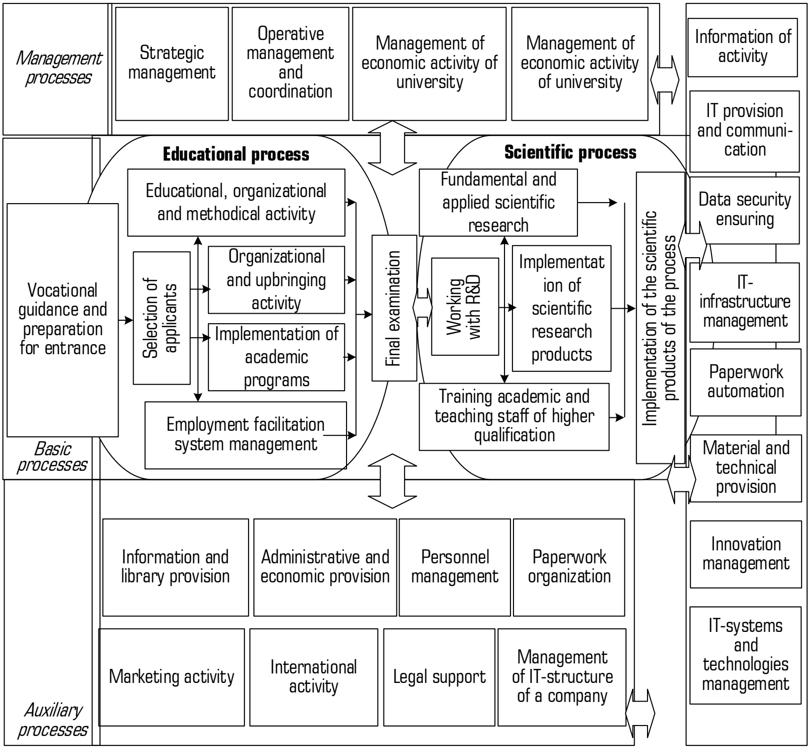

Channel / communication channels
Comprehension of damage MV2, $K^2_{MV2_i}$
Original text (OTP password)
FTC/ FTCH – flawed ciphertext
DCH/DCH – ciphertext damage
Decryption McEliece MCCS
$KU = G_X^{EC}$ – public key,
$KR = \{G^{EC}, X, P, D\}$ – private key
Encryption Niederreiter MCCS
$KU = H_X^{EC}$ – public key,
$KR = \{H^{EC}, X, P, D\}$ – private key
Damage MV2, $K^2_{MV2_i}$
Original text (OTP password)
Encryption McEliece MCCS
$KU = G_X^{EC}$ – public key,
$KR = \{G^{EC}, X, P, D\}$ – private key
Comparison of OTP passwords
Damage MV2, $K^1_{MV2_i}$
FTC/ FTCH – flawed ciphertext
DCH/DCH – ciphertext damage
Decryption Niederreiter MCCS
$KU = H_X^{EC}$ – public key,
$KR = \{H^{EC}, X, P, D\}$ – private key
Channel / communication channels
Comprehension of damage MV2, $K^1_{MV2_i}$

Fig. 4.31 Schematic block diagram of practical implementation of HCCSFC

Expression (4.4) makes it possible to evaluate the stability of the proposed McEliece and Niederreiter hybrid crypto-code systems on flawed codes.

4.7 THE USE OF ASYMMETRIC CRYPTO-CODE STRUCTURES IN THE SECURITY CONCEPT OF AN INNOVATIVE ACTIVE UNIVERSITY

The new paradigm fundamentally changes the culture of responsibility and the value system of a university as evidenced by the spread of managerial approach and the use of the principle of value for money in higher education systems around the world. Competitiveness and relevance of the university's existence are assessed mainly in accordance with its contribution to the economic development of countries and humanity as a whole. To adapt to the new paradigm, some adaptation is required – the adaptation of the university's relations with the surrounding society/core stakeholders, the adaptation of its internal processes, core values, and finding new innovative foundations for its development in today's environment. **Fig. 4.32** shows the relationship between management processes and the main functions of an innovative and active university, taking into consideration the development of e-education.


Management processes
Strategic management
Operative management and coordination
Management of economic activity of university
Management of economic activity of university
Information of activity
IT provision and communication
Data security ensuring
IT-infrastructure management
Paperwork automation
Material and technical provision
Innovation management
IT-systems and technologies management
Educational process
Scientific process
Educational, organizational and methodical activity
Organizational and upbringing activity
Implementation of academic programs
Employment facilitation system management
Vocational guidance and preparation for entrance
Selection of applicants
Final examination
Fundamental and applied scientific research
Working with R&D
Implementation of scientific research products
Training academic and teaching staff of higher qualification
Implementation of the scientific products of the process
Basic processes
Information and library provision
Administrative and economic provision
Personnel management
Paperwork organization
Marketing activity
International activity
Legal support
Management of IT-structure of a company
Auxiliary processes

⬡ **Fig. 4.32** Scheme of the interconnection of management processes and the main functions of an innovative and active university

The functioning safety of an innovative university is implemented at the following levels:

– at *the strategic level* – university authorities – the creation of conditions for the impossibility of making corruption changes in the guidelines on the organization of the educational process, providing basic public and communication services of the university's activities, conditions of students' life and transparency of rendering educational services. Ensuring effective control of keeping to the academic schedule at the university's faculties;

– at *the operational level* – faculty authorities, departments, and services involved in the system of service delivery – prevention of corrupt changes in the objectivity of students' assessment in the process of learning, accruing scholarships (grants, etc.). Organizing exams throughout the entire cycle of the educational process, creating conditions for effective monitoring of the implementation of the academic schedule for the specialities of a faculty, preventing corruption in departments and services of a university;

– at *the tactical level* – heads of departments – rising the level of objectivity of students' assessment in certain disciplines, creating the conditions of transparent students' choice of academic disciplines from the unit of an elective component of the educational process. Creating conditions for effective monitoring of the implementation of the academic schedule by teachers of departments.

The concept of security and corruption counteraction is presented in **Fig. 4.33, *a–c***.

Fig. 4.34 shows the variant of the block diagram of corporate information and education system (CIES) of an information active university, taking into consideration the basic functions of information resource (IR) management and security (IR IIAS) in the face of hybrid threats and possible corruption schemes. As a rule, CIES is formed based on web technologies that make it possible to meet the requirements of informativeness, openness, and accessibility to IR of CIES.

Therefore, in addition to ensuring the authenticity of the KCC-based IR of CIES, it is proposed to use commercial implementation of the crypto-code designs by McEliece and Niederreiter to ensure IR confidentiality and integrity. This approach will ensure not only the required level of crypto resistance under conditions of the emergence of a full-scale quantum computer, the speed of crypto-transformations at the level of block-symmetrical ciphers, reliability, but also counteraction to cyber book-marks based on encryption standards [135, 136]. The basics of practical construction of crypto-code designs by McEliece and Niederreiter on modified elliptical codes and flawed codes are considered in papers [153, 154].

Thus, the proposed approach to providing basic security services makes it possible to ensure the required level of security of the IR of CIES and to counteract modern cyber threats, both external and internal.

The conceptual synergistic security model of CIES (corporate information and educational system) of the IAU is based on particular models: advanced models of the CIES infrastructure and of an attacker, a synergistic threat model that makes it possible to assess security level.

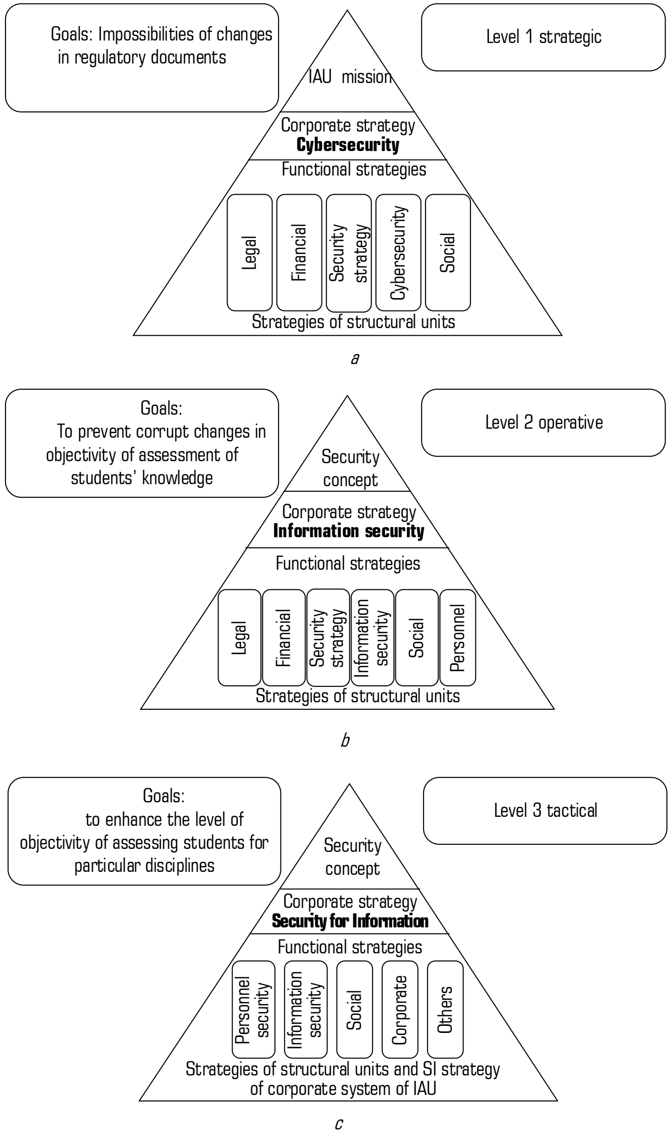
The improved model of the CIES infrastructure is described by the model:

$$G^{CIES} = \{\{O^{CIES}\}, \{L^{CIES}\}, \{I_A\}\}, \tag{4.5}$$

where $\{O^{CIES}\}$ is the set of environment objects describing the elements of the KIO infrastructure and their belonging to the levels of ISO/OSI model, $\{L^{CIES}\}$ is the set of relations between the elements of the infrastructure, determined by the adjacency matrix:

$$A^{CIES} = \left\| a_{ij}^{CIES} \right\|.$$

$\{I_A\}$ is the set of elements of information assets. Each element $I_{A_i} \in \{I_A\}$ is described by vector $I_{A_i} = \left(Type, A^C, A^I, A^A, A^{Av}\right)$. *Type* is the type of information assets, described by the set of basic values *Type*={*PID*, *StO*, *OI*, *YI*, *PD*, *SI*}, where *PID* is the payment documents, *StO* is the statistic reports, *OI* is the public information, *YI* is the management (regulatory information), *PD* is the personal data of CIES users, *SI* is the scientific information (know-how).



⬡ **Fig. 4.33** Concept of corruption counteraction:
a – strategic level; *b* – operational level; *c* – tactical level

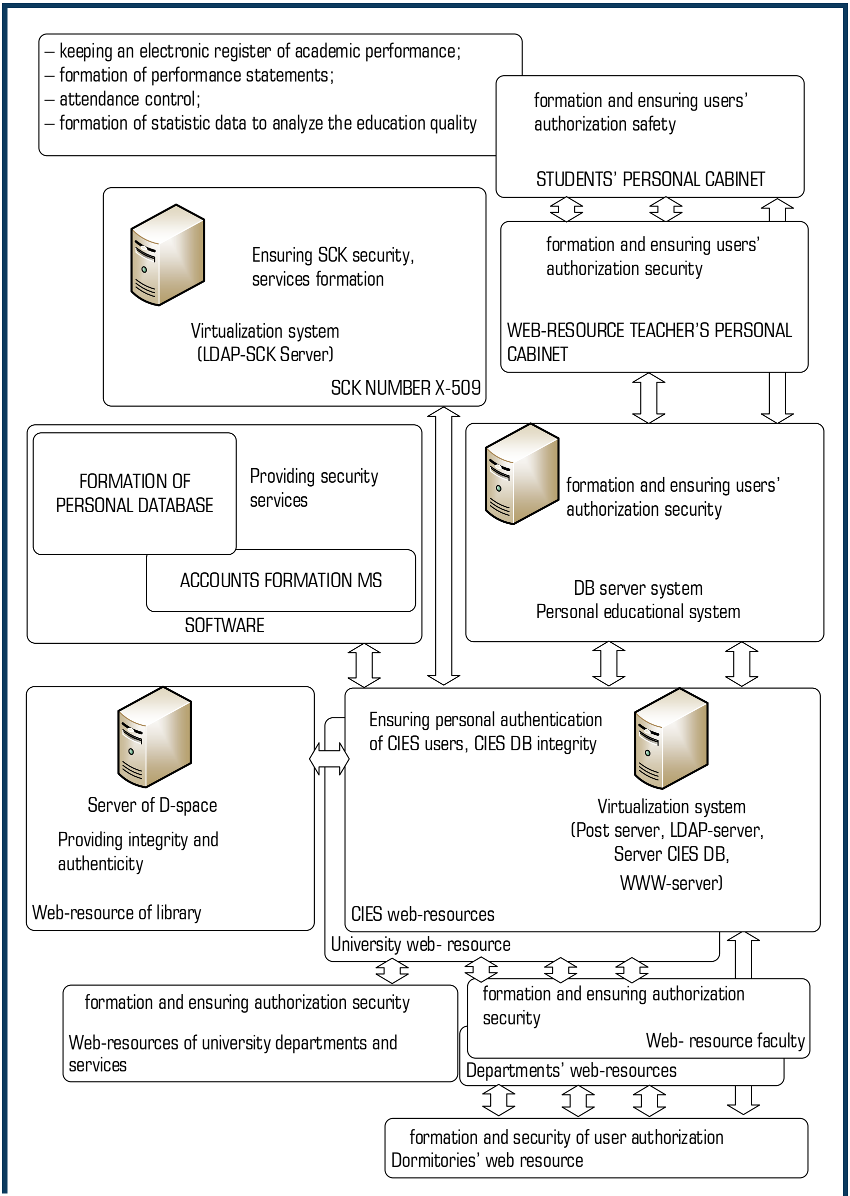

– keeping an electronic register of academic performance;
– formation of performance statements;
– attendance control;
– formation of statistic data to analyze the education quality
formation and ensuring users' authorization safety
STUDENTS' PERSONAL CABINET
Ensuring SCK security, services formation
Virtualization system (LDAP-SCK Server)
SCK NUMBER X-509
formation and ensuring users' authorization security
WEB-RESOURCE TEACHER'S PERSONAL CABINET
FORMATION OF PERSONAL DATABASE
Providing security services
ACCOUNTS FORMATION MS
SOFTWARE
formation and ensuring users' authorization security
DB server system
Personal educational system
Server of D-space
Providing integrity and authenticity
Web-resource of library
Ensuring personal authentication of CIES users, CIES DB integrity
Virtualization system (Post server, LDAP-server, Server CIES DB, WWW-server)
CIES web-resources
University web- resource
formation and ensuring authorization security
Web-resources of university departments and services
formation and ensuring authorization security
Web- resource faculty
Departments' web-resources
formation and security of user authorization
Dormitories' web resource

Fig. 4.34 A variant of the block diagram of CIES of an innovative and active university

A^C is privacy, A^I is integrity, A^A is authenticity, accessibility, A^A is continuity – the information properties to ensure. They accept the value of 1 if a property is necessary, 0 – otherwise.

Each element $O_l \in \left\{O^{CIES}\right\}$, is described by vector $O_l = \left\{Y^{CIES}, IO\right\}$, where Y^{CIES} is the level of information structure hierarchy, determined by set $Y^{CIES} = \{FL, NL, OSL, DBL, BL\}$, where *FL* is the physical level, *NL* is the network level, *OSL* is the level of operation systems (OS), *DBL* is the database management level, *BL* is the level of technical applications and servers. The following rule is used to indicate the type of connection and existing relation IO^R between information assets and environment objects:

$$IO^R = \left\| IO_{il}^R \right\|, \tag{4.6}$$

where IO_{il}^R displays the existence and the type of relations between the *i*-th information asset and the *l*-th environment object. In this case $\forall i \in \left\{I_A\right\}$, and $\forall l \in \left\{O^{CIES}\right\}$:

$$IO_{il}^R = \begin{cases} 0, \text{ no connection;} \\ cs, \text{ includes and stores;} \\ pt, \text{ processes and transfers;} \\ so, \text{ maintains functioning.} \end{cases}$$

The synergistic model of threats can be formally presented as:

$$ThM_{syn}^{CIES} = \left\{\left\{DF^{CIES}\right\}, \left\{T_{risk}\right\}, \left\{T_P\right\}, \left\{T_U\right\}, \left\{VH\right\}\right\}. \tag{4.7}$$

The set of the sources of CIES safety threats is represented by the tuple $DF^{SIES} = \left\{V^{NS}, V^{AS}\right\}$, in which V^{NS} is the class of natural threat sources, $V^{AS} = \left\{V^{ACS}, V^{AIS}, V^{ASI}\right\}$ is the class of anthropogenic threats, where V^{ACS} is the set of threats to cyber safety, V^{AIS} is the set of threats to information security, V^{ASI} is the set of threats to the safety of information. T_{risk} is the qualitative risk indicator, T_p is the set of basic terms of probability of implementation of at least one threat to the *j*-th asset, T_U is the set of basic terms of the magnitude of damage from the implementation of threat u_i, *VH* is the set of destructive states of the elements of the CIES infrastructure, which imply an undesirable and unplanned state of the CIES element, in which it got as a result of the implementation of one or several threats.

In order to have a synergistic effect of increasing the information security level, it is necessary to take into account the complexing of threats:

$$DF^{CIES} = \left\{V^{NS}\right\} \cup \left\{V^{AS}\right\},$$

where

$$\left\{V^{AS}\right\} = \left\{V^{ACS}\right\} \cap \left\{V^{AIS}\right\} \cap \left\{V^{ASI}\right\}, \tag{4.8}$$

where each element of the set of threats $DF_i \in \left\{DF^{CIES}\right\}$ can be represented by the following vector of values of $DF_i(T, T_p, pr_{ij}, r_{motiv})$, where *T* is the time of successful implementation of a threat, T_p is the set of basic terms of probability of implementation of at least one threat to the *j*-th asset,

pr_{ij} is the probability of implementation of at least one threat to the *j*-th asset, *i* is the threat, $\forall i \in n$, n is the number of threats, *j* is the information resource (asset), $\forall j \in m$, m is the number of assets; r_{motiv} is the probability of attacker's motivation to implement a threat.

However, the estimate of the probability of implementation of the *i*-th threat to the *j*-th asset will be determined taking into account the relations between the threat sources and CIES elements, which is assigned by matrix $A^{DF} = \left\| a_{ij}^{DF} \right\|$, dimensionality *n* on *m*, where *n* is the number of threats, *m* is the number of assets. For each *i*-th threat to the *j*-th asset, we determine the probability of implementation of pr_{ij} based on accumulated statistic data, characteristic of the given region and operation conditions (in the quantitative and/or qualitative form) or in an expert way.

The probability of the implementation of at least one threat to each asset is calculated according to the following formula:

$$p_{rj} = 1 - \prod_{i=1}^{m} \left(1 - pr_{ij}\right), \tag{4.9}$$

where p_{rj} is the probability of implementation of at least one threat to the *j*-th asset.

It is supposed that in case of implementation of at least one threat from set $V^{AS} = \left\{V^{ACS}, V^{AIS}, V^{ASI}\right\}$ to the *j*-th asset, the damage is equal to the cost of the asset based on detailing the assets and through the selection of actual threats:

$$q_j = u_j. \tag{4.10}$$

It is believed that threats can be implemented independently of each other, then the price of risk R_j for each *j*-th asset is determined from the following formula:

$$R_j = pr_{ij} \times q_j. \tag{4.11}$$

The full cost of risk is equal to the sum of costs of risk of all assets:

$$R_{full} = \sum_{j=1}^{n} R_j. \tag{4.12}$$

Thus, the probability of implementation of environment p_{rj} with the region of determining $P = [0,\ 1]$ will be assigned by the set of basic terms $T_p = \{$non-implemented, minimum, medium, high, critical$\} = \{\alpha_{x1}, \alpha_{x2}, \alpha_{x3}, \alpha_{x4}, \alpha_{x5}\}$.

The formal improved model of an attacker will be determined taking into consideration the proposals in papers [4, 34], in which the categories and actions of attackers are determined as:

$$G_{IA}^{CIES} = \left\{aid_i, T_{IA}, S_{\max_i}, pr_{ij}, r_{motiv}\right\}, \quad \forall i \in n, \quad \forall j \in m, \tag{4.13}$$

where $aid_i \in \left\{aid\right\}$ is the attacker's identifier, T_{IA} is the time of successful implementation of a threat, $S_{\max_i}$ is the probabilistic damage of a system, pr_{ij} is the probability of implementation of at least one threat to the *j*-th asset, *i* is the threat, $\forall i \in n$, *n* is the number of threats, *j* is the information resource (asset), $\forall j \in m$, *m* is the number of assets; r_{motiv} is the probability of motivation of an attacker to implement a threat.

To assess threats, we use a set of sources of threats, which include the sources of four types:

$$DF^{CIES} = \left\{V^{NS}, V^{AS}, TS, PI, NI\right\}, \tag{4.14}$$

where *TS* is the technical means and systems; *PI* is the deliberate attackers; *NI* is the non-deliberate attackers (offenders).

Thus, the proposed model makes it possible to take into consideration the complexing of threats, their synergy and hybridity, to form preventive measures based on the analysis of crucial threats and critical points in the CIES infrastructure.

Investigation of the properties of McEliece NCCS at EC and modified McEliece CCC at MEC. Let us estimate the parameters of asymmetric code-theoretic schemes using elliptic codes. Let us introduce the following notation:

– l_I – the length of the information sequence (block) arriving at the input of the code-theoretic scheme (in bits);

– l_K – public key length (in bits); l_{K+} – private key length (in bits);

– l_s – length of the codogram (in bits); O_K – the complexity of the formation of the codogram (the number of group operations); O_{SK} – c falsity of codogram decoding (number of group operations); O_{K+} – the complexity of solving the analysis problem (the number of group operations); K_C – residual compression ratio; K_f – flag compression ratio; *s* – number of pieces of flawed text; *u*(*n*), *v*(*r*) – positive flawed key numbers; *z*(*m*) – rounds of flaw; L_0 – source text length; L_{DT} – the length of the flawed text.

To construct the graphs, the following conditional abbreviations (prefixes) were used: ukh/udh – hybrid CCC with shortened MEC/hybrid CCC with elongated MEC; uk – MCCC with shortened MEC; ud – MCCC with extended MEC.

When calculating the parameters of cryptosystems, Galois fields were used: for McEliece code theotretic scheme (CTS) – $GF(2^{10})$; for MCCC with shortened/extended MEC – $GF(2^6)$; for hybrid CCC – $GF(2^4)$.

Let us carry out a comparative analysis of the parameters of the McEliece asymmetric code-theoretic scheme (ACTS) using *EC*, with the parameters of the modified McEliece MCCC on the *MEC*.

To estimate *the length of the information sequence* (*in bits*) arriving at the input of the MCCC with an algebraic (*n*, *k*, *d*)-code over $GF(2^m)$, we use the expressions:

– for ACTS on the *EC*: $l_I = k \times m$;

– for MCCC on shortened *MEC* codes: $l_I = 1/2k \times m$;

– for MCCC on extended *MEC* codes: $l_I = k \times m$.

The complexity of decoding the codogram is determined by the expressions: for ACTS on the *EC*: $O_{SK} = 2 \times n^2 + k^2 + 4t^2 + (t^2 + t - 2)^2/4$;

– for MCCC on shortened *MEC*:

$$O_{SK} = 2\left(2\sqrt{q} + q + 1 - 1/2k\right)^2 + 1/2k^2 + 4t^2 + \left(t^2 + t - 2\right)^2 \Big/ 4;$$

– for MCCC on extended *MEC*:

$$O_{SK}=2\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)+k^2+4t^2+\left(t^2+t-2\right)^2/4.$$

The complexity of solving the problem of analysis (decoding) is given by the expressions: for ACTS on *EC*:

$$O_{K+}=N_{coverings}\, n\times r,$$

where

$$N_{\text{coverings}}\geq\frac{C_n^{\rho\cdot t}}{C_{n-k}^{\rho\cdot t}}=\frac{n(n-1)\ldots(n-\rho\cdot t-1)}{(n-k)(n-k-1)\ldots(n-k-\rho\cdot t-1)},\quad t=\left[(d-1)/2\right].$$

The potential resistance of the cryptosystem is determined by the value ρ×*t*, and the noise immunity of the system – (1–ρ)×*t*. For MCCC on shortened codes:

$$O_{K+}=N_{\text{coverings}}\times\left(2\sqrt{q}+q+1-1/2k\right)\times r;$$

– for MCCC on long codes:

$$O_{K+}=N_{\text{coverings}}\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)\times r.$$

Table 4.8 and **Fig. 4.35** shows the dependence of the complexity of cracking and the complexity of coding for various *EC* rates (*MEC*).

Table 4.9 and **Fig. 4.36** shows the dependences of the volume of open key data for various indicators of durability.

⬢ **Table 4.8** Pivot Chart of Hack Difficulty and Coding Difficulty for Various EC Baudrates

lg(l_s)	**0.5**	**0.75**	**0.5(*ud*)**	**0.75(*ud*)**	**0.5(*uk*)**	**0.75(*uk*)**
1	4.75	12.1	15.6	18.23	19.12	19.82
2	10.52	21.76	32.47	35.67	38.63	39.18
3	18.22	33.17	43.75	51.61	56.88	58.03
4	21.42	51.75	59.43	72.81	78.92	80.52
5	38.77	61.09	68.26	87.32	94.91	104.56
6	54.13	78.37	**101.72**	**112.46**	**120.83**	**128.79**
7	82.14	83.72	156.75	164.72	182.39	189.74
8	165.84	179.13	223.64	231.57	276.27	287.33
9	358.33	371.09	421.97	428.63	459.81	476.52
10	**672.37**	**684.94**	716.41	722.26	783.46	794.28

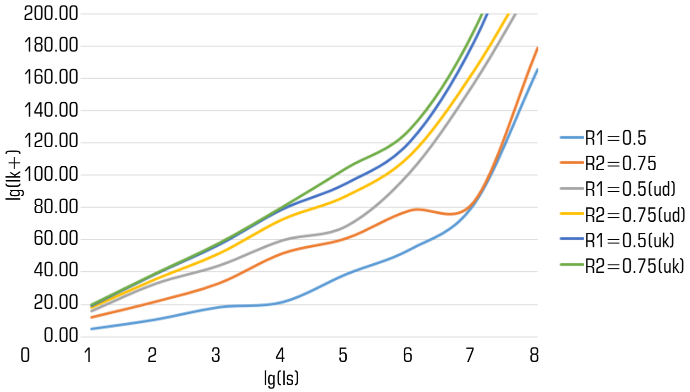


Fig. 4.35 Summary diagram of hacking complexity and coding complexity for different *EC* rates (*MEC*)

Table 4.9 Dependencies of the volume of open key data for various indicators of durability

$\lg(l_{k+})$	***R***					
	0.5	**0.75**	**0.5(*ud*)**	**0.75(*ud*)**	**0.5(*uk*)**	**0.75(*uk*)**
5	30	87	240	602	968	799
20	2278137	4351076	926137	987234	1034682	1897092
35	**12329538**	**14097276**	**4253109**	**5237688**	**6126273**	**6832018**
50	22541273	77520337	43076332	60122407	8602376	7027160

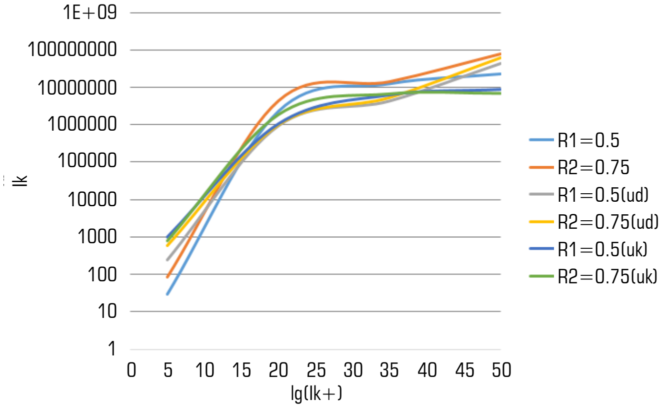


Fig. 4.36 Dependencies of the volume of open key data for various indicators of durability

Analysis of the presented results **Table 4.10** clearly demonstrates how the increase in the relative data transmission rate is obtained: the volume of key data in systems based on short/long codes is half that of a conventional NCCS.

Table 4.10 shows the results of studies of the capacitive characteristic for software implementation on the field power.

● **Table 4.10** Dependence of the software implementation speed on the field power (the number of group operations)

Cryptosystems	**2^5**	**2^6**	**2^7**	**2^8**	**2^9**	**2^{10}**
CCC McEliece on *EC*	10018042	18048068	32847145	47489784	63215578	**82467897**
MCCC McEliece on shortened *MEC*	10007947	**17787431**	28595014	44079433	61974253	79554764
MCCC McEliece on extended *MEC*	11156138	**18561228**	33210708	48297112	65171690	84051337

The resulting **Table 4.10** shows the number of group operations of the software implementation of the CCC, depending on the field strength. It can be seen that if for the implementation of McEliece CCC in field GF(2^{10}), 82.5×10^6 group operations are required, then the implementation of MNCCS on shortened/extended MECs in field GF(2^6) requires 17.7 – 18.6×10^6 group operations, i.e. 4.5 times less.

Let us carry out a comparative analysis of the parameters of McEliece MCCC on *MEC* (shortened/elongated) and with the parameters of HCCCFC on the basis of McEliece HCCCFC on *MEC*. *The length of the information sequence* (in bits) arriving at the input of the cryptosystem with the CC is determined by the following expression: for hybrid crypto-coded construction on flawed code (HCCCFC) on shortened codes:

$$I_I = I_z^c + I_z^f,$$

where $I_z^c = K_c \times L + 1/K_f \times s$ – the length of the flawed text; $I_z^f = L + u \times s$ – damage length; $s = \left[\left(L_0 - L_{DT} \right) / L_{DT} \right]$ – number of pieces of damaged text, $K_C = 1 - K_f \approx 0.758$ – compression ratio of the remainder (defective text) (while u=8, v=3, z=5); $K_f = \left(2 - 2^{v-u+1} \right) / u \approx 0.242$ – flag compression ratio (damage) (while u=8, v=3, z=5); $z = \left(\log\left(u \times L \right) - 7 \right) / \log\left(1/K_C \right)$ – required to randomize the MV2 cipher, the number of conversion rounds allowed. For HCCCFC on extended *MEC*: $I_I = 1/2k \times m + I_z^c + I_z^f$.

Table 4.11 and **Fig. 4.37** shows the results of studies of the complexity of the formation of a cryptogram in various *GF*(2^m).

The length of the codogram (in bits) is determined by the expressions: for HCCCFC on shortened *MEC*:

$$I_S = \left(2\sqrt{q} + q + 1 - 1/2k \right) \times m;$$

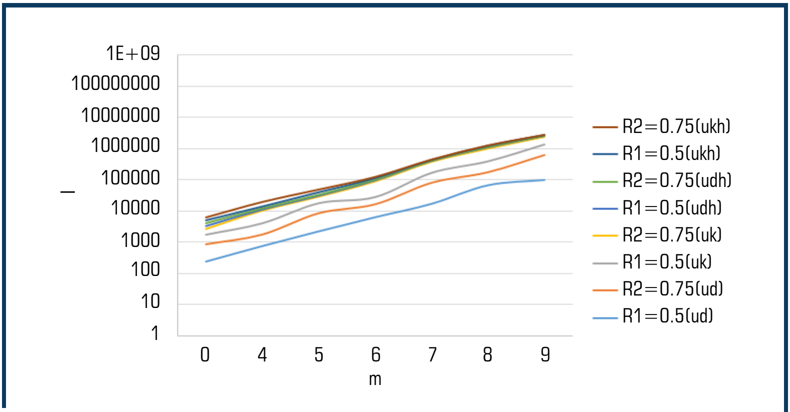
for HCCCFC for extended *MEC*:

$$I_s = \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times m.$$

Table 4.12 and **Fig. 4.38** shows the results of studies of the complexity of decoding a cryptogram in various *GF*(2*^m^*).

⬢ **Table 4.11** Dependence of the complexity of the formation of a cryptogram in various *GF*(2^m)

***GF*(2*^m^*)**	***R***							
	0.5(*ud*)	**0.75(*ud*)**	**0.5(*uk*)**	**0.75(*uk*)**	**0.5(*udh*)**	**0.75(*udh*)**	**0.5(*ukh*)**	**0.75(*ukh*)**
3	242	603	817	968	643	780	923	998
4	760	980	2140	6282	**905**	**1085**	**1563**	**5125**
5	2241	6121	8706	11461	1863	2450	6137	8282
6	**6348**	**9830**	**10722**	**60760**	6273	7016	9183	10341
7	17092	61751	83000	210170	16582	15985	16563	16925
8	67016	105265	207422	605005	65278	65450	66137	68282
9	98765	510780	710920	1018079	95327	96037	97134	97841



⬡ **Fig. 4.37** Dependence of the complexity of the formation of a cryptogram in various *GF*(2^m)

Analysis of the **Table 4.11**, **4.12** and **Fig. 4.37**, **4.38** showed that the use of defective codes and a further decrease in the power of the Galois field leads to a significant decrease in the complexity of the formation (by about 12 times) and decoding (by about 20 times) of the cryptogram.

Table 4.12 Dependence of the complexity of decoding a cryptogram in various *GF*(2*^m^*)

***GF*(2*^m^*)**	***R***							
	0.5(*ud*)	**0.75(*ud*)**	**0.5(*uk*)**	**0.75(*uk*)**	**0.5(*udh*)**	**0.75(*udh*)**	**0.5(*ukh*)**	**0.75(*ukh*)**
1	78	81	82	96	148	153	1568	1621
2	456	457	457	556	835	897	6112	9624
3	1024	1168	1280	5127	1240	1307	12283	14817
4	7672	8232	11028	23674	**5224**	**11937**	**34673**	**225017**
5	21073	42082	78634	277830	12348	25597	95088	1246572
6	**103862**	**281472**	**760553**	**5220573**	123548	127137	1316373	4383507

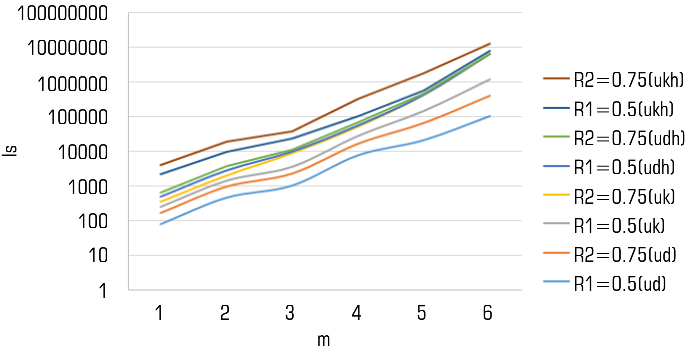


Fig. 4.38 Dependence of the complexity of decoding a cryptogram in various *GF*(2*^m^*)

The complexity of solving the problem of analysis (decoding) is defined by the expressions: for HCCCFC *on shortened MEC*:

$$O_{K+}=N_{\text{coverings}}\times\left(2\sqrt{q}+q+1-1/2k\right)\times r+N_F \text{ or } \left(N_K\right),$$

where $N_F \approx \left({K_C}^{z}/2^{1-{K_C}^{z+1}}\right)\times|F|, K_C$=97/128, $|F|$ – total length of output flags (damages) (bits) – with the remainder known to the attacker (damaged text) and given flags (damages), with an unknown key – $N_K \approx 2^{1190\times z}$, z=16; for HCCCFC for extended *MEC*:

$$O_{K+}=N_{\text{coverings}}\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)\times r+N_F \text{ or } \left(N_K\right).$$

Table 4.13 and **Fig. 4.39** shows the results of studies of the complexity of cracking and the complexity of coding for different rates *R* in different *GF*(2^m). **Table 4.14** and **Fig. 4.40** shows the results of studies of the dependence of the volume of open key data of HCCCFC per month for various indicators of persistence.

Table 4.13 The complexity of cracking and the complexity of coding for different rates *R*

lg(l_s)	***R***							
	0.5(*ud*)	**0.75(*ud*)**	**0.5(*uk*)**	**0.75(*uk*)**	**0.5(*udh*)**	**0.75(*udh*)**	**0.5(*ukh*)**	**0.75(*ukh*)**
1	15.6	18.23	19.12	19.82	7.21	9.17	12.54	14.56
2	32.47	35.67	38.63	39.18	21.46	23.72	27.48	29.82
3	43.75	51.61	56.88	58.03	31.68	33.83	37.38	38.43
4	59.43	72.81	78.92	80.52	**41.72**	**42.27**	**47.48**	**58.23**
5	68.26	87.32	94.91	104.56	56.63	58.91	62.86	66.53
6	**101.72**	**112.46**	**120.83**	**128.79**	72.32	74.79	89.5	97.71

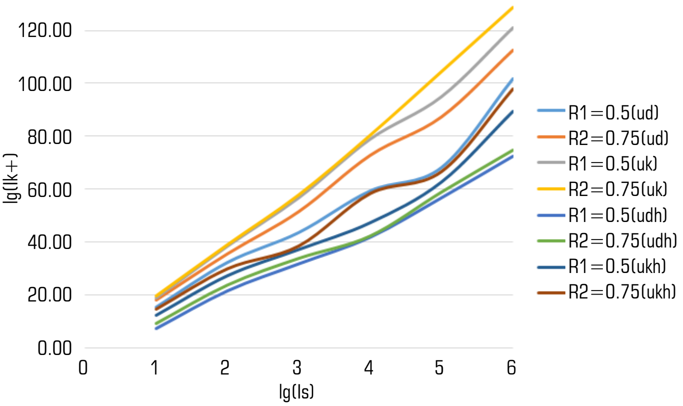


Fig. 4.39 Summary diagram of the complexity of cracking and the complexity of the coding of the HCCCFC for different rates of the MEC

Table 4.14 Dependences of the volume of open key data of the HCCCFC for various indicators of durability

lg(l_{k+})	**0.5(*ud*)**	**0.75(*ud*)**	**0.5(*uk*)**	**0.75(*uk*)**	**0.5(*udh*)**	**0.75(*udh*)**	**0.5(*ukh*)**	**0.75(*ukh*)**
5	240	602	968	799	812	827	853	898
20	926137	987234	1034682	1897092	87531	95019	312560	402843
35	**4253109**	**5237688**	**6126273**	**6832018**	**421108**	**650389**	**957648**	**1121732**
50	43076332	60122407	8602376	7027160	1032562	2340561	3867228	4218394

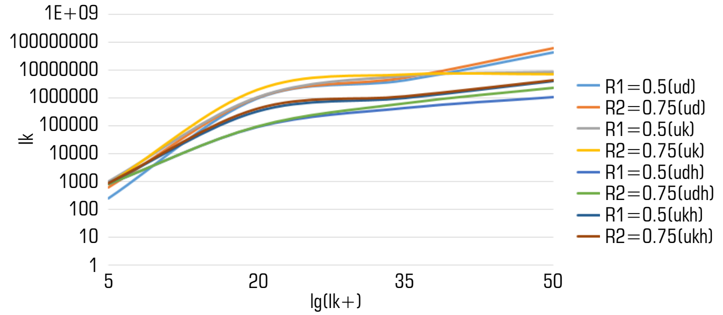


Fig. 4.40 Dependences of the volume of open key data of the HCCCFC for various indicators of durability

Table 4.15 shows the results of studies of the capacitive characteristic for software implementation on the field power.

Table 4.15 Dependence of the software implementation speed on the field power (the number of group operations)

CCC	**2^4**	**2^5**	**2^6**	**2^7**	**2^8**	**2^9**	**2^{10}**
CCC shortened *MEC*	8293075	10007947	**17787431**	28595014	44079433	61974253	79554764
MCCC on extended *MEC*	8506422	11156138	**18561228**	33210708	48297112	65171690	84051337
HCCCFC on extended *MEC*	**5612316**	7900315	14892945	25565274	42279183	58963778	76564173
HCCCFC on shortened *MEC*	**5942627**	7905257	14682411	25595014	42116327	58468143	75474764

As in the study, MCCC received a significant decrease in open key data for the HCCCFC, which leads to a total increase in the relative transmission rate.

A natural continuation of our research, obviously, should be testing the statistical characteristics of the proposed crypto-code structures in order to obtain objective traditional data on cryptographic strength.

To carry out statistical studies of the stability of the cryptosystems under study, we will use the NIST STS 822 package [155].

The research results are presented in **Table 4.16**.

Table 4.16 demonstrates that, despite the decrease in the Galois field power to *GF*(2^6) for MCCC and *GF*(2^4) for HCCCFC, the statistical characteristics of such crypto-code constructions turned out to be at least no worse than the traditional McEliece CTS on *GF*(2^{10}).

All cryptosystems passed 100 % of the NIST tests, and the best result was shown by the HCCCFC at shortened months: 155 out of 189 tests passed at the level of 0.99, which is 82 % of the total number of tests. At the same time, the traditional McEliece CTS on $GF(2^{10})$ showed 149 tests at the level of 0.99.

● **Table 4.16** Statistical security research results

Algorithm	**The number of tests in which more than 99 % of the sequences passed testing**	**The number of tests in which more than 96 % of the sequences passed testing**	**The number of tests in which less than 96 % of the sequences passed the test**
CTS McEliece *EC*	149 (78,83 %)	189 (100 %)	0 (0 %)
MCCC McEliece on shortened *MEC*	151 (79,89 %)	189 (100 %)	0 (0 %)
MNCCS McEliece on extended *MEC*	152 (80,42 %)	189 (100 %)	0 (0 %)
HCCCFC on McEliece on extended *MEC*	153 (80,95 %)	189 (100 %)	0 (0 %)
HCCCFC on McEliece on shortened *MEC*	155 (82 %)	189 (100 %)	0 (0 %)

The conducted studies of the proposed modifications of the crypto-code structures of McEliece and Niederreiter allow us to consider the synergy of their application to provide basic security services. The used noise-resistant algebraic geometric codes provide the required level of reliability ($P_{error}=10^{-9}$–10^{-12}), the formed asymmetric systems provide the level of cryptographic resistance (10^{35} elementary group operations), which in the post-quantum period allows their use in post-quantum security protocols. The encoding/decoding rate in the proposed modified crypto-code constructions is comparable to the rate of crypto-transformations in symmetric cryptoalgorithms with a key length of 2^{128}–2^{256}, which in the post-quantum crypto-period is twice as fast as the BSW of post-quantum cryptography (key length 2^{512}). The use of defective codes in modified CCCs allows the formation of hybrid CCCs of McEliece and Niederreiter, in which the approach to constructing such systems is fundamentally different (ensuring symmetric cryptography provides cryptographic strength).

In **Fig. 4.41** presents a block diagram of synergy based on the use of the proposed CCCs on *MEC*/flawed codes.

The use of flawed codes in hybrid McEliece and Niederreiter CCCs significantly (20 times) reduces the energy capacity of the practical implementation of the proposed encoding/decoding algorithms. This approach expands the range of use of the CCC to ensure the safety, reliability and efficiency of information resources in the post-quantum period, in the protection systems of critical infrastructure facilities.

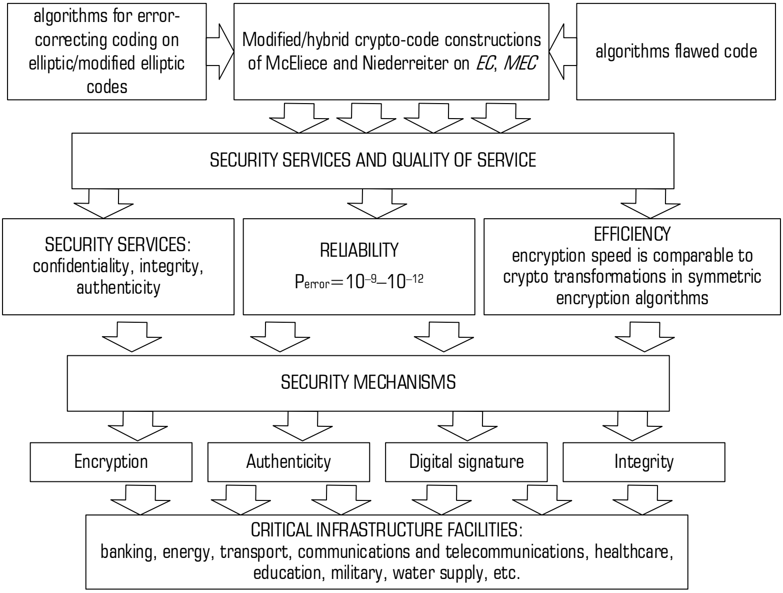

algorithms for error-correcting coding on elliptic/modified elliptic codes
Modified/hybrid crypto-code constructions of McEliece and Niederreiter on *EC*, *MEC*
algorithms flawed code
SECURITY SERVICES AND QUALITY OF SERVICE
SECURITY SERVICES: confidentiality, integrity, authenticity
RELIABILITY
$P_{error}=10^{-9}$–10^{-12}
EFFICIENCY
encryption speed is comparable to crypto transformations in symmetric encryption algorithms
SECURITY MECHANISMS
Encryption
Authenticity
Digital signature
Integrity
CRITICAL INFRASTRUCTURE FACILITIES:
banking, energy, transport, communications and telecommunications, healthcare, education, military, water supply, etc.

Fig. 4.41 Structural diagram of the synergistic effect of using McEliece and Niederreiter CCC on *MEC*/flawed codes in post-quantum security protocols

Thus, the use of modified CCC (hybrid) crypto-code constructions of McEliece and Niederreiter on modified elliptic codes (shortened/extended) in systems with defective codes provides the required level of security with minimal energy costs (construction of CCC over the field *GF*(2^4) in a wide range of standards for information transmission channels, storage of information resources, formation of special security mechanisms: encryption, authenticity, integrity, digital signature – all this allows us to assert that crypto-code constructions provide the synergy of building security systems.

CONCLUSIONS

1. The main types of models used in modeling the behavior of intelligent agents was discussed. The use of models of different classes together with the consideration of various aspects of the behavior of agents in conditions of cyber conflict makes it possible to obtain a synergistic effect of the proposed modeling methodology. The originality of the approach associated with the introduction into consideration of the concept of the contour of business processes as an integral object to be protected. Consideration of the business processes loops of the organizational and technological system and the loops of business processes of the cybersecurity system can be considered as another condition for the manifestation of the synergy of the processes under consideration. The idea of the spatio-temporal structure of the model basis was proposed by the authors, that reflects not only the distribution of the set of models over the corresponding levels of the proposed methodology, but also sets the sequence of their interaction. This approach can be considered as the closure of a set of conditions for the manifestation of the synergistic properties of the proposed methodology for modeling conflict-cooperative interaction between the parties to a cyber conflict.

2. As a result of research based on the proposed mathematical models of data protection in the social network, determining the resilience of the data protection system and the resilience of the system to possible influences, on the basis of which an objective assessment of the balance between information security threats and specific parameters of the social network interaction, external influences and protection measures and the amount of data protected. The application of the developed models to ensure the protection of information and user data in social networks will allow a new look at existing social networks (modernization of their structure, parameters, user interaction) and create new social networks that will provide more reliable security of user data while maintaining usage parameters. The developed mathematical model for assessing the stability of the information protection system in social networks is based on the analysis of the parameters of the behavior of the protection system during and after external influences on the data protection system taking into account the dynamics of change of influence parameters. The model allows to carry out research of parameters of protection of system and to take necessary measures for improvement of system of protection of the information taking into account nonlinear interaction of elements of system of protection and external influences.

3. Practical aspects of the methodology for constructing post-quantum algorithms for asymmetric McEliece and Niederreiter cryptosystems based on algebraic and defective codes can significantly reduce the energy costs for implementation, while ensuring the required level of cryptographic strength of the system as a whole. The security concept of a corporate information and educational system based on the construction of an adaptive information protection system allows ensuring the security of information resources and the quality of service for users of an active innovative university in the face of targeted modern threats. A significant increase in the speed of systems has been achieved (at least 20 times in the speed of formation of a cryptogram), which allows the use of conventional personal computing equipment for cryptographic protection of information by such systems, while ensuring the required level of cryptographic stability in the post-quantum period.

REFERENCES

1. Riley, M., Elgin, B., Lawrence, D., Matlack, C. (2014). Missed alarms and 40 million stolen credit card numbers: How target blew it. Available at: http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data Last accessed: 30.03.2016
2. M-trends 2016 (2016). Mandaint: A FireEye Company. Technical report. Available at: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-mtrends-2016.pdf
3. Jajodia, S., Noel, S. (2010) Advanced cyber attack modeling analysis and visualization. Technical report, DTIC Document. Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a516716.pdf
4. Qin, X., Lee, W. (2004). Attack plan recognition and prediction using causal networks. Proceedings of 20th Annual Computer Security Applications Conference. Tucson, 370–379. doi: http://doi.org/10.1109/csac.2004.7
5. Xie, P., Li, J. H., Ou, X., Liu, P., Levy, R. (2010). Using bayesian networks for cyber security analysis. Proceedings of 2010 IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Chicago, 211–220. doi: http://doi.org/10.1109/dsn.2010.5544924
6. Fava, D. S., Byers, S. R., Yang, S. J. (2008). Projecting Cyberattacks Through Variable-Length Markov Models. IEEE Transactions on Information Forensics and Security, 3 (3), 359–369. doi: http://doi.org/10.1109/tifs.2008.924605
7. Stotz, A., Sudit, M. (2007). Information fusion engine for real-time decisionmaking: A perceptual system for cyber attack tracking. Proceedings of 2007 10th International Conference on Information Fusion. Quebec, 1–8. doi: http://doi.org/10.1109/icif.2007.4408113
8. Wang, B., Cai, J., Zhang, S., Li, J. (2010). A network security assessment model based on attack-defense game theory. Proceedings of 2010 International Conference on Computer Application and System Modeling (ICCASM). Taiyuan, 3, V3–639. doi: http://doi.org/10.1109/iccasm.2010.5620536
9. Grunewald, D., Liitzenberger, M., Chinnow, J., Bye, R., Bsufka, K., Albayrak, S. (2011). Agent-based network security simulation. Proceedings of The 10th International Conference on Autonmous Agents and Multiagent Systems, 3, 1325–1326.
10. Moskal, S., Wheeler, B., Kreider, D., Kuhl, M. E., Yang, S. J. (2014). Context model fusion for multistage network attack simulation. Proceedings of Military Communications Conference (MILCOM). Baltimore, 158–163. doi: http://doi.org/10.1109/milcom.2014.32
11. Moskal, S., Kreider, D., Hays, L., Wheeler, B., Yang, S. J., Kuhl, M. (2013) Simulating attack behaviors in enterprise networks. Proceedings of 2013 IEEE Conference on Communications and Network Security (CNS). National Harbor, 359–360. doi: http://doi.org/10.1109/cns.2013.6682726
12. Sheyner, O., Haines, J., Jha, S., Lippmann, R., Wing, J. M. (2002) Automated generation and analysis of attack graphs. Proceedings of 2002 IEEE Symposium on Security and Privacy. Berkeley, 273–284. doi: http://doi.org/10.1109/secpri.2002.1004377

13. Jha, S., Sheyner, O., Wing, J. (2002). Two formal analyses of attack graphs. Proceedings of 2002 15th IEEE Computer Security Foundations Workshop. Cape Breton, 49–63. doi: http://doi.org/10.1109/csfw.2002.1021806
14. Moskal, S. F. (2016). Knowledge-based Decision Making for Simulating Cyber Attack Behaviors. Rochester Institute of Technology.
15. Kotenko, I., Doynikova, E. (2015). The CAPEC based generator of attack scenarios for network security evaluation. Proceedings of 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). Warsaw, 1, 436–441. doi: http://doi.org/10.1109/idaacs.2015.7340774
16. Yevseiev, S., Milov, O., Milevskyi, S., Voitko, O., Kasianenko, M., Melenti, Y. et. al. (2020). Development and analysis of game-theoretical models of security systems agents interaction. Eastern-European Journal of Enterprise Technologies, 2 (4 (104)), 15–29. doi: http://doi.org/10.15587/1729-4061.2020.201418
17. Milov, O., Kostyak, M., Milevsky, S., Pogasiy, S. (2019). Methods for modeling agent behavior in information and communication systems. Control, Navigation and Communication Systems. Academic Journal, 6 (58), 63–70. doi: http://doi.org/10.26906/sunz.2019.6.063
18. Yevseiev, S., Karpinski, M., Shmatko, O., Romashchenko, N., Gancarczyk, T., Falat, P. (2019). Methodology of the cyber security threats risk assessment based on the fuzzy-multiple approach. 19th International Multidisciplinary Scientific GeoConference SGEM2019, Informatics, Geoinformatics and Remote Sensing. Sofia, 437–444. doi: http://doi.org/10.5593/sgem2019/2.1/s07.057
19. Yevseiev, S., Aleksiyev, V., Balakireva, S., Peleshok, Y., Milov, O., Petrov, O. et. al. (2019). Development of a methodology for building an information security system in the corporate research and education system in the context of university autonomy. Eastern-European Journal of Enterprise Technologies, 3 (9 (99)), 49–63. doi: http://doi.org/10.15587/1729-4061.2019.169527
20. Yevseiev, S., Ponomarenko, V., Ponomarenko, V., Rayevnyeva, O., Rayevnyeva, O. (2017). Assessment of functional efficiency of a corporate scientificeducational network based on the comprehensive indicators of quality of service. Eastern-European Journal of Enterprise Technologies, 6 (2 (90)), 4–15. doi: http://doi.org/10.15587/1729-4061.2017.118329
21. Sun, R. (2007). The importance of cognitive architectures: an analysis based on CLARION. Journal of Experimental & Theoretical Artificial Intelligence 19 (2), 159–193. doi: http://doi.org/10.1080/09528130701191560
22. Gilbert, N. (2004). Agent-based social simulation: dealing with complexity. Tech. rep. University of Surrey.
23. Carley, K. M., Prietula, M. J., Lin, Z. (1998). Design versus cognition: The interaction of agent cognition and organizational design on organizational performance. Journal of Artificial Societies and Social Simulation 1 (3). Available at: http://jasss.soc.surrey.ac.uk/1/3/4.html
24. Helbing, D., Balletti, S. (2011). How to do agent-based simulations in the future: From modeling social mechanisms to emergent phenomena and interactive systems design. Working Paper 11-06-024. Santa Fe Institute. Available at: https://www.santafe.edu/research/results/working-papers/how-to-do-agent-based-simulations-in-the-future-fr
25. Axelrod, R., Tesfatsion, L., Tesfatsion, L., Judd, K. L. (Eds.) (2006). A guide for newcomers to agent-based modeling in the social sciences. Handbook of Computational Economics, Vol. 2:

Agent-Based Computational Economics. Chap. Appendix A. Elsevier, 164–1659. doi: http://doi.org/10.1016/s1574-0021(05)02044-7

26. Nilsson, N. J. (1977). A production system for automatic deduction. Technical Note 148. Stanford. Available at: http://www.ai.sri.com/pubs/files/743.pdf
27. Chao, Y. R. (1968). Language and symbolic systems. Cambridge University Press, 260. Available at: http://services.cambridge.org/us/academic/subjects/languages-linguistics/english-language-and-linguistics-general-interest/language-and-symbolic-systems?format=PB&isbn=9780521094573
28. Ishida, T. (1994). Parallel, Distributed and Multiagent Production Systems, vol. 878 of Lecture Note in Computer Science. Springer. doi: http://doi.org/10.1007/3-540-58698-9
29. Bordini, R. H., Hübner, J. F., Wooldridge, M. (2007). Programming Multi-Agent Systems in AgentSpeak using Jason. Wiley Series in Agent Technology. John Wiley & Sons, 292.
30. Dignum, F., Kinny, D., Sonenberg, L. (2002). From desires, obligations and norms to goals. Cognitive Science Quarterly, 2 (3-4), 407–430. Available at: http://dspace.library.uu.nl/handle/1874/19827
31. Cohen, P. R., Levesque, H. J. (1990). Intention is choice with commitment. Artificial Intelligence, 42 (2-3), 213–261. doi: http://doi.org/10.1016/0004-3702(90)90055-5
32. Adam, C., Gaudou, B. (2016). BDI agents in social simulations: a survey. The Knowledge Engineering Review, 31 (3), 207–238. doi: http://doi.org/10.1017/s0269888916000096
33. Pereira, D., Oliveira, E., Moreira, N., Sarmento, L. (2005). Towards an architecture for emotional bdi agents. EPIA'05: Proceedings of 12th Portuguese Conference on Artificial Intelligence. Springer. doi: http://doi.org/10.1109/epia.2005.341262
34. Jiang, H., Vidal, J. M. (2006). From rational to emotional agents. In: Proceedings of the AAAI Workshop on Cognitive Modeling and Agent-based Social Simulation. AAAI Press.
35. Kennedy, W. G.; Heppenstall, A. J., Crooks, A. T., See, L. M., Batty, M., (Eds.) (2012). Modelling human behaviour in agent-based models. Agent-Based Models of Geographical Systems. Springer, 167–179. doi: http://doi.org/10.1007/978-90-481-8927-4_9
36. Kollingbaum, M. J. (2005). Norm-Governed Practical Reasoning Agents. University of Aberdeen. Available at: https://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.415494
37. Dignum, F. (1999). Autonomous agents with norms. Artificial Intelligence and Law, 7 (1), 69–79. doi: http://doi.org/10.1023/a:1008315530323
38. Castelfranchi, C., Dignum, F., Jonker, C. M., Treur, J. (2000). Deliberate normative agents: Principles and architecture. Intelligent Agents VI, Agent Theories, Architectures, and Languages. Proceedings 6th International Workshop, ATAL'99. Orlando, 364–378. doi: http://doi.org/10.1007/10719619_27
39. Conte, R., Castelfranchi, C. (1995). Cognitive and Social Action. Taylor & Francis, 224. doi: http://doi.org/10.4324/9780203783221
40. Sun, R.; Lukose, D., Shi, Z. (Eds.) (2009). Cognitive architectures and multi-agent social simulation. Multi-Agent Systems for Society. Springer-Verlag, 7–21. doi: http://doi.org/10.1007/978-3-642-03339-1_2
41. Card, S. K., Newell, A., Moran, T. P. (1983). The Psychology of Human-Computer Interaction. Hillsdale: L. Erlbaum Associates Inc., 448. doi: http://doi.org/10.1201/9780203736166

42. Byrne, M. D.; Sears, A., Jacko, J. A. (Eds.) (2007). Cognitive architecture. The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies and Emerging Applications. CRC Press, 93–114. doi: http://doi.org/10.1201/9781410615862.ch5
43. Sun, R., Peterson, T., Sessions, C. (2002). Beyond simple rule extraction: acquiring planning knowledge from neural networks. Proceedings of WIRN'01. Springer, 288–300. doi: http://doi.org/10.1007/978-1-4471-0219-9_32
44. Laird, J. E. (2012). The SOAR Cognitive Architecture. Cambridge: MIT Press. doi: http://doi.org/10.7551/mitpress/7688.001.0001
45. Attiah, A., Chatterjee, M., Zou, C. C. (2018). A Game Theoretic Approach to Model Cyber Attack and Defense Strategies. 2018 IEEE International Conference on Communications (ICC). doi: http://doi.org/10.1109/icc.2018.8422719
46. Alpcan, T., Baser, T. (2006). An intrusion detection game with limited observations. Proc. 12th Int. Symp. on Dynamic Games and Applications. Available at: https://wenku.baidu.com/view/07f2933031126edb6f1a10f9.html
47. Security measurement – white paper (2006). Available at: http://www.psmsc.com/Downloads/TechnologyPapers/SecurityWhitePaper_v3.0.pdf
48. He, W., Xia, C., Wang, H., Zheng, C., Ji, Y. (2008). A game theoretical attack-defense model oriented to network security risk assessment. International Conference on Computer Science and Software Engineering. Wuhan, 498–504. doi: http://doi.org/10.1109/csse.2008.1651
49. Yazar, Z. (2002). A qualitative risk analysis and management tool. CRAMM. SANS Institute. Available at: https://www.sans.org/reading-room/whitepapers/auditing/paper/83
50. Aigbokhaevbolo, O. (2011). Application of Game Theory to Business Strategy in Undeveloped Countries: A Case for Nigeria. Journal of Social Sciences, 27 (1), 1–5. doi: http://doi.org/10.1080/09718923.2011.11892900
51. Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., Hubaux, J.-P. (2013). Game theory meets network security and privacy. ACM Computing Surveys, 45 (3), 1–39. doi: http://doi.org/10.1145/2480741.2480742
52. Akinwumi, D. A., Iwasokun, G. B., Alese, B. K., Oluwadare, S. A. (2018). A review of game theory approach to cyber security risk management. Nigerian Journal of Technology, 36 (4), 1271–1285. doi: http://doi.org/10.4314/njt.v36i4.38
53. Kesselman, A., Leonardi, S. (2012). Game-theoretic analysis of Internet switching with selfish users. Theoretical Computer Science, 452, 107–116. doi: http://doi.org/10.1016/j.tcs.2012.05.029
54. Akella, A., Karp, R., Papadimitriou, C., Seshan, S., Shenker, S. (2002). Selfish behavior and the stability of the internet: A game theoretic analysis of TCP. Proceedings of SIGCOMM 2002. doi: http://doi.org/10.1145/633025.633037
55. Alpcan, T., Basar, T., Dey, S. (2004). A power control game based on outage probabilities for multicell wireless data networks. Proceedings of the 2004 American Control Conference. doi: http://doi.org/10.23919/acc.2004.1386817
56. Bencsth, B., Buttyn, L., Vajda, I. (2003). A game-based analysis of the client puzzle approach to defend against dos attacks. Soft- COM 2003 11th International conference on software, telecommunications and computer networks, 763–767.

57. Michiardi, P., Molva, R. (2002). Core: A collaborative reputation mechanism to enforce node co-operation in mobile ad hoc networks. 6th IEIP Communications and Multimedia Security Conference. doi: http://doi.org/10.1007/978-0-387-35612-9_9
58. Kodialam, M., Lakshman, T. V. (2003). Detecting network intrusions via sampling: A game theoretic approach. IEEE IN- EOCOMM 2003. San Francisco. doi: http://doi.org/10.1109/infcom.2003.1209210
59. Patchat, A., Park, J.-M. (2004). A Game Theoretic Approach to Modeling Intrusion Detection in Mobile Ad Hoc Networks. Proceedings of the 2004 IEEE Workshop on Information Assurance and Security. United States Military Academy. West Point. doi: http://doi.org/10.1109/iaw.2004.1437828
60. Alazzawe, A., Nawaz, A., Bayaraktar, M. M. (2006). Game theory and intrusion detection systems.
61. Hamilton, S. N., Miller, W. L., Ott, A., Saydjari, O. S. (2002). Challenges in applying game theory to the domain of information warfare. Proceedings of the 4th Information survivability workshop (ISW-2001/2002).
62. Hamilton, S. N., Miller, W. L., Ott, A., Saydjari, O. S. (2002). The role of game theory in information warfare. Proceedings of the 4th information survivability workshop (ISW- 2001/2002).
63. Liu, P., Zang, W., Yu, M. (2005). Incentive-based modeling and inference of attacker intent, objectives, and strategies. ACM Transactions on Information and System Security, 8 (1), 78–118. doi: http://doi.org/10.1145/1053283.1053288
64. Nguyen, K. C., Alpcan, T., Basar, T. (2009). Stochastic games for security in networks with interdependent nodes. 2009 International Conference on Game Theory for Networks. Istanbul. doi: http://doi.org/10.1109/gamenets.2009.5137463
65. Nguyen, K. C., Alpcan, T., Basar, T. (2009). Security Games with Incomplete Information. 2009 IEEE International Conference on Communications. Dresden. doi: http://doi.org/10.1109/icc.2009.5199443
66. Chen, Z. (2007). Modeling and defending against internet worm attacks. Georgia Institute of Technology.
67. Hryshchuk, R. V. (2013). Dyferentsialno-ihrovi modeli ta metody modeliuvannia protsesiv kibernapadu. Kyiv, 411.
68. Bursztein, E., Goubault-Larrecq, J. (2007). A Logical Framework for Evaluating Network Resilience Against Faults and Attacks. Advances in Computer Science – ASIAN 2007. Computer and Network Security, 4846, 212–227. doi: http://doi.org/10.1007/978-3-540-76929-3_20
69. Sun, W., Kong, X., He, D., You, X. (2008). Information Security Problem Research Based on Game Theory. 2008 International Symposium on Electronic Commerce and Security. Guangzhou. doi: http://doi.org/10.1109/isecs.2008.147
70. Hansman, S., Hunt, R. (2005). A taxonomy of network and computer attacks. Computers & Security, 24 (1), 31–43. doi: http://doi.org/10.1016/j.cose.2004.06.011
71. Ma, C. Y. T., Yau, D. K. Y., Lou, X., Rao, N. S. V. (2013). Markov Game Analysis for Attack-Defense of Power Networks Under Possible Misinformation. IEEE Transactions on Power Systems, 28 (2), 1676–1686. doi: http://doi.org/10.1109/tpwrs.2012.2226480

72. Milov, O., Yevseiev, S., Ivanchenko, Y., Milevskyi, S., Nesterov, O., Puchkov, O. et. al. (2019). Development of the model of the antagonistic agents behavior under a cyber conflict. Eastern-European Journal of Enterprise Technologies, 4 (9 (100)), 6–19. doi: http://doi.org/10.15587/1729-4061.2019.175978
73. Gordon, L. A., Loeb, M. P., Lucyshyn, W., Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. Journal of Accounting and Public Policy, 34 (5), 509–519. doi: http://doi.org/10.1016/j.jaccpubpol.2015.05.001
74. Huang, C. D., Behara, R. S. (2013). Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. International Journal of Production Economics, 141 (1), 255–268. doi: http://doi.org/10.1016/j.ijpe.2012.06.022
75. Alguliyev, R., Imamverdiyev, Y., Sukhostat, L. (2018). Cyber-physical systems and their security issues. Computers in Industry, 100, 212–223. doi: http://doi.org/10.1016/j.compind.2018.04.017
76. Cárdenas, A. A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y., Sastry, S. (2011). Attacks against process control systems. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security – ASIACCS'11, 355–366. doi: http://doi.org/10.1145/1966913.1966959
77. Gollmann, D. (2013). Security for Cyber-Physical Systems. Mathematical and Engineering Methods in Computer Science, 12–14. doi: http://doi.org/10.1007/978-3-642-36046-6_2
78. Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., Sastry, S. (2009). Challenges for securing cyber physical systems. Workshop on future directions in cyber-physical systems security.
79. Pfleeger, C. P., Pfleeger, S. L. (2006). Security in Computing. Prentice Hall, 880.
80. Cebula, J. J., Young, L. R. (2010). A taxonomy of operational cyber security risks. Technical report, DTIC Document.
81. Kang, D.-J., Lee, J.-J., Kim, S.-J. Park, J.-H. (2009). Analysis on cyber threats to SCADA systems. 2009 Transmission & Distribution Conference & Exposition: Asia and Pacific. Seoul. doi: http://doi.org/10.1109/td-asia.2009.5357008
82. Nicholson, A., Webber, S., Dyer, S., Patel, T., Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. Computers & Security, 31 (4), 418–436. doi: http://doi.org/10.1016/j.cose.2012.02.009
83. Guide for conducting risk assessments (2012). NIST. doi: http://doi.org/10.6028/nist.sp.800-30r1
84. Cyber threat source descriptions. US-CERT. Available at: https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions
85. Milov, O., Korol, O., Khvostenko, V. (2019). Development of the classification of the cyber security agents bounded rationality. Control, Navigation and Communication Systems. Academic Journal, 4 (56), 82–90. doi: http://doi.org/10.26906/sunz.2019.4.082
86. Yevseiev, S. (2017). Intruder model of access rights in the automated banking system based on a synergistic approach. Naukovo-tekhnichnyi zhurnal «Informatsiyna bezpeka», 2 (26), 110–120.
87. Kravets, D. (2009). Feds: Hacker disabled offshore oil platforms' leak-detection system. Available at: https://www.wired.com/2009/03/feds-hacker-dis/

88. Chattopadhyay, A., Prakash, A., Shafique, M. (2017). Secure Cyber-Physical Systems: Current trends, tools and open research problems. Design, Automation & Test in Europe Conference & Exhibition (DATE). Lausanne. doi: http://doi.org/10.23919/date.2017.7927154
89. Dell Security (2016). Annual Threat Report. Available at: https://www.netthreat.co.uk/assets/assets/dell-security-annual-threat-report-2016-white-paper-197571.pdf
90. Walker, J. J. (2012). Cyber Security Concerns for Emergency Management. Emergency Management. doi: http://doi.org/10.5772/34104
91. Ali, N. S. (2016). A four-phase methodology for protecting web applications using an effective real-time technique. International Journal of Internet Technology and Secured Transactions, 6 (4), 303. doi: http://doi.org/10.1504/ijitst.2016.10003854
92. Park, K.-J., Zheng, R., Liu, X. (2012). Cyber-physical systems: Milestones and research challenges. Computer Communications, 36 (1), 1–7. doi: http://doi.org/10.1016/j.comcom.2012.09.006
93. State of the Phish: An in-depth look at user awareness (2020). Available at: https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/proofpoint/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf
94. Goel, S., Chen, V. (2005). Information security risk analysis – a matrix-based approach. Proceedings of the Information Resource Management Association (IRMA) International Conference. San Diego.
95. Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. Computers & Security, 25 (7), 522–538. doi: http://doi.org/10.1016/j.cose.2006.08.004
96. Blackwell, C. (2010). A security ontology for incident analysis. Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research – CSIIRW'10. doi: http://doi.org/10.1145/1852666.1852717
97. Hryshchuk, R., Yevseiev, S. (2017). Methodology of building a system for providing information security of bank information in automated banking systems. Ukrainian Scientific Journal of Information Security, 23 (3), 204–214. doi: http://doi.org/10.18372/2225-5036.23.12095
98. Pollock, G. M., Atkins, W. D., Schwartz, M. D., Chavez, A. R., Urrea, J. M., Pattengale, N. et. al. (2010). Modeling and simulation for cyber-physical system security research, development and applications. doi: http://doi.org/10.2172/1028942
99. Ahmad, R., Yunos, Z. (2012). A dynamic cyber terrorism framework. International Journal of Computer Science and Information Security, 10 (2), 149–158.
100. Loukas, G., Gan, D., Vuong, T. (2013). A taxonomy of cyber attack and defence mechanisms for emergency management networks. 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). San Diego. doi: http://doi.org/10.1109/percomw.2013.6529554
101. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0 (2014). National Institute of Standards and Technology. Available at: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-10
102. Hughes, J., Cybenko, G. (2014). Three tenets for secure cyber-physical system design and assessment. Cyber Sensing 2014. doi: http://doi.org/10.1117/12.2053933

103. Buchyk, S. (2016). The methodology of analysis of risks of tree that identifiers the state informative resources. Ukrainian Information Security Research Journal, 18 (1), 81–89. doi: http://doi.org/10.18372/2410-7840.18.10116
104. Yevseiev, S., Rzayev, K., Mammadova, T., Samedov, F., Romashchenko, N. (2018). Classification of cyber cruise of informational resources of automated banking systems. Cybersecurity: Education, Science, Technique, 2, 47–67. doi: http://doi.org/10.28925/2663-4023.2018.2.4767
105. Barabash, O., Laptiev, O., Tkachev, V., Maystrov, O., Krasikov, O., Polovinkin, I. (2020). The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information. International Journal of Emerging Trends in Engineering Research, 8 (8), 4133–4139. doi: http://doi.org/10.30534/ijeter/2020/17882020
106. Benson, V., Saridakis, G., Tennakoon, H., Ezingeard, J. N. (2015). The role of security notices and online consumer behaviour: An empirical study of social networking users. International Journal of Human-Computer Studies, 80, 36–44. doi: http://doi.org/10.1016/j.ijhcs.2015.03.004
107. Mvungi, B., Iwaihara, M. (2015). Associations between privacy, risk awareness, and interactive motivations of social networking service users, and motivation prediction from observable features. Computers in Human Behavior, 44, 20–34. doi: http://doi.org/10.1016/j.chb.2014.11.023
108. Barabash, O., Laptiev, O., Kovtun, O., Leshchenko, O., Dukhnovska, K., Biehun, A. (2020). The Method dynavic TF-IDF. International Journal of Emerging Trends in Engineering Research, 8 (9), 5713–5718. doi: http://doi.org/10.30534/ijeter/2020/130892020
109. Yevseiev, S., Laptiev, O., Lazarenko, S., Korchenko, A., Manzhul, I. (2021). Modeling the protection of personal data from trust and the amount of information on social networks. EUREKA: Physics and Engineering, 1, 24–31. doi: http://doi.org/10.21303/2461-4262.2021.001615
110. Laptiev, O., Savchenko, V., Kotenko, A., Akhramovych, V., Samosyuk, V. Shuklin, G., Biehun, A. (2021) Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security, 13 (1), 1–14.
111. Obidin, D., Ardelyan, V., Lukova-Chuiko, N., Musienko, A. (2017). Estimation of Functional Stability of Special Purpose Networks Located on Vehicles. Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD). Kyiv: National Aviation University, 167–170. doi: http://doi.org/10.1109/apuavd.2017.8308801
112. Korotin, S., Kravchenko, Y., Starkova, O., Herasymenko, K., Mykolaichuk, R. (2019). Analytical determination of the parameters of the self-tuning circuit of the traffic control system on the limit of vibrational stability. International Scientific-Practical Conference Problems of Infocommunications Science and Technology. PIC S&T'2019 – Proceedings. Kyiv, 471–476. doi: http://doi.org/10.1109/picst47496.2019.9061256
113. Rakushev, M., Permiakov, O., Tarasenko, S., Kovbasiuk, S., Kravchenko, Y., Lavrinchuk, O. (2019). Numerical Method of Integration on the Basis of Multidimensional Differential-Taylor Transformations. Proceedings of the IEEE International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S&T'2019 – Proceedings. Kyiv, 675–678. doi: http://doi.org/10.1109/picst47496.2019.9061339
114. Kravchenko, Y., Leshchenko, O., Dakhno, N., Trush, O., Makhovych, O. (2019). Evaluating the effectiveness of cloud services. IEEE International Conference on Advanced Trends in

Information Theory. ATIT'2019 – Proceedings. Kyiv, 120–124. doi: http://doi.org/10.1109/atit49449.2019.9030430

115. Sobchuk, V., Pichkur, V., Barabash, O., Laptiev, O., Kovalchuk, I., Zidan, A. (2020). Algorithm of control of functionally stable manufacturing processes of enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings. Kyiv, 206–211.

116. Savchenko, V., Laptiev, O., Kolos, O., Lisnevskyi, R., Ivannikova, V., Ablazov, I. (2020) Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings. Kyiv, 246–251.

117. Chen, P. A., Desmet, L., Huygens, C. (2019) Study on Advanced Persistent Threats. Communications and Multimedia Security. Berlin Heidelberg: Springer, 63–72. doi: http://doi.org/10.1007/978-3-662-44885-4_5

118. Freeman, L. C., Borgatti, S. P., White, D. R. (1991). Centrality in valued graphs: A measure of betweenness based on network flow. Social Networks, 13 (2), 141–154. doi: http://doi.org/10.1016/0378-8733(91)90017-n

119. Yevseiev, S., Korolyov, R., Tkachov, A., Laptiev, O., Opirskyy, I., Soloviova, O. (2020). Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period. International Journal of Advanced Trends in Computer Science and Engineering, 9 (5), 8725–8729. doi: http://doi.org/10.30534/ijatcse/2020/261952020

120. Laptiev, O., Stefurak, O., Polovinkin, I., Barabash, O., Savchenko, V., Zelikovska, O. (2020). The method of improving the signal detection quality by accounting for interference. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings. Kyiv, 172–176.

121. Korchenko, A., Breslavskyi, V., Yevseiev, S., Zhumangalieva, N., Zvarych, A., Kazmirchuk, S. et. al. (2021). Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency. Eastern-European Journal of Enterprise Technologies, 1 (2 (109)), 14–23. doi: http://doi.org/10.15587/1729-4061.2021.225346

122. Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., Scarfone, K. (2016). Guide for cybersecurity event recovery. NIST. doi: http://doi.org/10.6028/nist.sp.800-184

123. Security requirements for cryptographic modules (2001). Available at: https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf Last accessed: 01.02.2020

124. Cichonski, J., Franklin, J. M., Bartock, M. (2017). Guide to LTE security. doi: http://doi.org/10.6028/nist.sp.800-187

125. Hryshchuk, R., Yevseiev, S., Shmatko, A. (2018). Construction methodology of information security system of banking information in automated banking systems. Vienna: Premier Publishing, 284. doi: http://doi.org/10.29013/r.hryshchuk_s.yevseiev_a.shmatko.cmissbiabs.284.2018

126. Lohachab, A., Lohachab, A., Jangra, A. (2020). A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. Internet of Things, 9, 100174. doi: http://doi.org/10.1016/j.iot.2020.100174

127. Petrenko, K., Mashatan, A., Shirazi, F. (2019). Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial

organization. Journal of Information Security and Applications, 46, 151–163. doi: http://doi.org/10.1016/j.jisa.2019.03.007

128. Aggarwal, S., Chaudhary, R., Aujla, G. S., Kumar, N., Choo, K.-K. R., Zomaya, A. Y. (2019). Blockchain for smart communities: Applications, challenges and opportunities. Journal of Network and Computer Applications, 144, 13–48. doi: http://doi.org/10.1016/j.jnca.2019.06.018
129. Bobok, I., Kobozeva, A., Maksymov, M., Maksymova, O. (2016). Checking the Integrity of CCTV Footage in Real Time at Nuclear Facilities. Nuclear and Radiation Safety, 2 (70), 68–72. doi: http://doi.org/10.32918/nrs.2016.2(70).14
130. Kobozeva, A. A., Bobok, I. I., Garbuz, A. I. (2016). General Principles of Integrity Checking of Digital Images and Application for Steganalysis. Transport and Telecommunication Journal, 17 (2), 128–137. doi: http://doi.org/10.1515/ttj-2016-0012
131. Bobok, I. I. (2018). Steganalysis method for detection of the hidden communication channel with low capacity. Telecommunications and Radio Engineering, 77 (18), 1597–1604. doi: http://doi.org/10.1615/telecomradeng.v77.i18.20
132. Kobozeva, A. A., Bobok, I. I., Batiene, L. E. (2018). Steganoanalytical Method Based on the Analysis of Singular Values of Digital Image Matrix Blocks. Problemele Energeticii Regionale, 3 (38), 156–168. doi: http://doi.org/10.5281/zenodo.2222384
133. Kobozeva, A. A., Bobok, I. I., Grygorenko, S. M. (2020). Method for Detecting of Clone Areas in a Digital Image under Conditions of Additional Attacks. Journal of Signal Processing Systems, 92 (1), 55–69. doi: http://doi.org/10.1007/s11265-019-01449-6
134. Evseev, S., Abdullayev, V. (2015). Monitoring algorithm of two-factor authentication method based on passwindow system. Eastern-European Journal of Enterprise Technologies, 2 (2 (74)), 9–16. doi: http://doi.org/10.15587/1729-4061.2015.38779
135. Yevseiev, S., Hryhorii, K., Liekariev, Y. (2016). Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system. Eastern-European Journal of Enterprise Technologies, 6 (4 (84)), 11–23. doi: http://doi.org/10.15587/1729-4061.2016.86175
136. Yevseiev, S., Kots, H., Minukhin, S., Korol, O., Kholodkova, A. (2017). The development of the method of multifactor authentication based on hybrid cryptocode constructions on defective codes. Eastern-European Journal of Enterprise Technologies, 5 (9 (89)), 19–35. doi: http://doi.org/10.15587/1729-4061.2017.109879
137. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S. et. al. (2018). Practical implementation of the Niederreiter modified cryptocode system on truncated elliptic codes. Eastern-European Journal of Enterprise Technologies, 6 (4 (96)), 24–31. doi: http://doi.org/10.15587/1729-4061.2018.150903
138. Milov, O., Yevseiev, S., Ivanchenko, Y., Milevskyi, S., Nesterov, O., Puchkov, O. et. al. (2019). Development of the model of the antagonistic agents behavior under a cyber conflict. Eastern-European Journal of Enterprise Technologies, 4 (9 (100)), 6–19. doi: http://doi.org/10.15587/1729-4061.2019.175978
139. Sidelnikov, V. M. (2002). Kriptografiia i teoriia kodirovaniia. Moskovskii universitet i razvitie kriptografii v Rossii. Moscow, 1–22.
140. Sidelnikov, V. M., Shestakov, S. O. (1992). O sisteme shifrovaniia, postroennoi na osnove obobshhennyh kodov Rida-Solomona. Diskretnaia matematika, 4 (3), 57–63.

141. Anohin, M. I., Varnovskii, N. P., Sidelnikov, V. M., Jashhenko, V. V. (1997). Kriptografiia v bankovskom dele. Moscow: MIFI.

142. Yevseiev, S., Tsyhanenko, O., Gavrilova, A., Guzhva, V., Milov, O., Moskalenko, V. et. al. (2019). Development of Niederreiter hybrid crypto-code structure on flawed codes. Eastern-European Journal of Enterprise Technologies, 1 (9 (97)), 27–38. doi: http://doi.org/10.15587/1729-4061.2019.156620

143. Tsyhanenko, O., Yevseiev, S., Milevskyi, S. (2019). Using the Flawed Codes In Niederreiter Crypto-Code Structure. Short Paper Proceedings of the 1st International Conference on Intellectual Systems and Information Technologies (ISIT 2019). Odessa, 17–19.

144. McEliece, R. J. (1978). A Public-Key Criptosystem Based on Algebraic Theory. DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, 114–116.

145. Niederreiter, H. (1986). Knapsack-Type Cryptosystems and Algebraic Coding Theory. Problems of Control and Information Theory, 15, 19–34.

146. Mak-Viliams, F., Sloen, N. (1979). Teoriia kodov, ispravliaiuschikh oshibki. Moscow: Sviaz, 744.

147. Muterr, V. M. (1990). Osnovy pomekhoustoichivoi teleperedachi informatsii. Leningrad: Energoatomizdat. Leningr. otd-nie, 288.

148. Mishhenko, V. A., Vilanskii, Yu. V. (2007). Ushherbnye teksty i mnogokanalnaia kriptografiia. Minsk: Enciklopediks.

149. Mischenko, V. A., Vilanskii, Iu. V., Lepin, V. V.; Mischenko, V. A. (Ed.) (2007). Kriptograficheskii algoritm MV2. Minsk: Entsiklopediks, 176.

150. Meyer, D. (2016). Time is running out for this popular online security technique. FORTUNE. Available at: http://fortune.com/2016/07/26/nist-sms-two-factor/

151. Hackett, R. (2016). You're implementing this basic security feature all wrong. FORTUNE. Available at: http://fortune.com/2016/06/27/two-factor-authentication-sms-text/

152. McBride, T., Ekstrom, M., Lusty, L., Sexton, J., Townsend, A. (2017) Data Integrity: Recovering from Ransomware and Other Destructive Events. NIST Special Publication 1800-11. Available at: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/di-nist-sp1800-11a-draft.pdf

153. Yevseiev, S., Korol, O., Kots, H. (2017). Construction of hybrid security systems based on the crypto-code structures and flawed codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (88)), 4–21. doi: http://doi.org/10.15587/1729-4061.2017.108461

154. Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O. et. al. (2020). Development of methodological foundations for designing a classifier of threats to cyber-physical systems. Eastern-European Journal of Enterprise Technologies, 3 (9 (105)), 6–19. doi: http://doi.org/10.15587/1729-4061.2020.205702

155. Rukhin, A., Soto, J. (2000). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22. doi: http://doi.org/10.6028/nist.sp.800-22

Edited by
Serhii Yevseiev, Volodymyr Ponomarenko, Oleksandr Laptiev, Oleksandr Milov

SYNERGY OF BUILDING CYBERSECURITY SYSTEMS

Monograph

PC TECHNOLOGY CENTER
Published in May 2021
Enlisting the subject of publishing No. 4452 – 10.12.2012
Address: Shatylova dacha str., 4, Kharkiv, Ukraine, 61165