

Ruslan HRYSHCHUK, Serhii YEVSEIEV, Alexander SHMATKO

CONSTRUCTION METHODOLOGY OF INFORMATION SECURITY SYSTEM OF BANKING INFORMATION IN AUTOMATED BANKING SYSTEMS

Monograph



PREMIER
Publishing

Premier Publishing s.r.o.

Vienna 2018

Hryshchuk R., Yevseiev, S. Shmatko A.

Construction methodology of information security system of banking information in automated banking systems : monograph – Vienna.: Premier Publishing s.r.o., 2018. – 284 p.

ISBN 978-3-903197-50-3

The monograph presents modern methodology of building information security systems of banking information systems. The methodology is based on a new concept of building a threat model, constructed on synergistic principles. As a result, for the first time a three-tier security model of strategic management of banking information technologies has being built for the automated banking system. This system takes into account threats of cybersecurity, information security and threats for the security of banking information at the same time.

Special attention should be given to the methods proposed in the monograph to ensure the confidentiality, integrity and authenticity of information in banking information systems. In contrast to the known ones, the proposed methods are built on hybrid cryptographic structures with redundant codes. Principles of the methods are mathematical models of hybrid cryptocodic constructions with using asymmetric crypto-modified McEliece and Niederreiter codes and modified geometric codes.

The book is full of applied examples that confirm the validity of the developed methods and the adequacy of the proposed models.

In this way a comprehensive solution has been proposed from a systemic position on the base of a synergistic approach, to ensure the information security of banking information systems. The proposed methodology opens up the new methods to building security systems for the critical information infrastructures of the state and business which is new in terms of security and a rational in terms of money spent

The results are proposed to be used at planning measures to ensure the information security of automated banking systems for minimization of risks from new threats to the security of banking information.

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.

Subscribe to print 28/11/2018. Format 60×90¹/₁₆.

Offset Paper. Garinitura Arno. Conv. Pec. liter. 11. Edition of 500 copies.

Typeset in Berling by Ziegler Buchdruckerei, Linz, Austria.

Printed by Premier Publishing s.r.o. Vienna,

Vienna, Austria on acid-free paper.

Am Gestade 1, 1010 Vienna, Austria

pub@ppublishing.org, ppublishing.org

ISBN 978-3-903197-50-3

© R. Hryshchuk, S. Yevseiev, A. Shmatko 2018.

© Premier Publishing s.r.o. Vienna, 2018.

Contents

List of Conditions	7
INTRODUCTION	9
CHAPTER 1. State of the art analysis	11
1.1 Review of the literature on problem	11
1.1.1 <i>Analysis of the nature and content of information security problems in the current development of science and technology</i>	11
1.1.2 <i>Investigation of the role and place of information security system of banking information in automated banking systems</i>	23
1.1.3 <i>Research infrastructure facilities threats automated banking systems</i>	28
1.1.4 <i>Analysis of current state services and mechanisms for cryptographic protection of banking information</i>	39
1.2 Substantiation of the dissertation.....	46
1.3 Formulation of the problem	49
1.4 Conclusions of the first chapter	50
References in Chapter 1	51
CHAPTER 2. Development conceptual foundations of information security of banking information in the automated banking system	57
2.1 Developing the concept of building a synergetic model of banking information security threats in automated banking systems.....	57
2.2 The formalization of the principles of construction components threats branch banking information security, information security, cyber security, information security.....	65
2.3 The formalization of the problem of evaluation generalized index of banking information security in automated banking systems	70
2.3.1 <i>Improving the infrastructure of automated banking system</i>	70

2.3.2	<i>Development of a conceptual model of synergistic threats to information security of banking information in automated banking systems</i>	78
2.3.3	<i>Improving the offending model based on a synergistic approach to the assessment of threats to information security, cyber security, and information security</i>	81
2.3.4	<i>Improving evaluation model of banking security in automated banking systems</i>	87
2.4	Conclusions of the second section	90
	References in Chapter 2	91

CHAPTER 3. Development approaches to security banking services in automated banking system on hybrid crypto-code designs from unprofitable codes . . .98

3.1	Setting properties crypto-code systems geometrical codes	98
3.1.1	<i>Setting properties asymmetric crypto code of McEliece and Niederreiter Elliptic codes</i>	105
3.1.2	<i>Development of a method of masking elliptical codes</i>	110
3.1.3	<i>Develop methods modified elliptical codes</i>	112
3.1.4	<i>Research on properties of modified elliptical cryptographic codes</i>	129
3.2	Develop methods to ensure the integrity and confidentiality of banking information in automated banking systems on hybrid designs crypto code of unprofitable codes	136
3.2.1	<i>Research on the cryptographic properties of building codes unprofitable</i>	136
3.2.2	<i>The development of mathematical models of hybrid crypto-code constructions based on asymmetric crypto-modified code of McEliece and Niederreiter on modified geometrical codes</i>	147
3.2.3	<i>Studying the properties of hybrid crypto-code designs on unprofitable codes</i>	160
3.3	Develop methods to ensure the authenticity of the bank in automated banking systems based on two-factor authentication hybrid crypto code structures with unprofitable codes	168
3.3.1	<i>Research protocols two-factor authentication</i>	168
3.3.2	<i>Analysis of the threats that are relevant for today's two factor authentication protocols</i>	172

3.3.3 Use two-factor authentication based on PassWindow and analysis of safety.	176
3.3.4 Research methods for constructing OTP-password.	180
3.3.5 Development of two factor authentication protocol on hybrid designs crypto code of unprofitable codes.	184
3.3.6 Studying the properties of the proposed method of two-factor authentication.	188
3.4 Conclusions of the third section.	189
References in Chapter 3.	190

CHAPTER 4. Development effectiveness evaluation approach to investment banking in information security in automated banking system ... 196

4.1 Development of evaluation method investment information security of banking information in terms of simultaneous action of threats to information security, cyber security and banking information.	196
4.1.1 Development of composite indicator of investment in the system of banking information security in automated banking systems.	196
4.1.2 The development of methods of cryptosystems stability evaluation based on entropy method for assessing the randomness of the original sequence.	206
4.2 Develop comprehensive measure of service quality evaluation objects automated banking system to ensure the safety of bank information.	212
4.3 The findings of the fourth section.	224
References in Chapter 4.	225

CHAPTER 5. Verification and investigation of developed models and methods. Construction methodology of information security system of banking information in the automated banking system.231

5.1 Comparative analysis of the transfer banking informa- tion efficiency in automated banking systems developed through comprehensive measure of evaluating the quality of service objects automated banking system to ensure the safety of bank information.	231
---	-----

5.2 Generalization of the results: the methodology of synthesis and analysis of the proposed models and methods of information security of banking information.	235
5.3 Experiment	252
5.4 Conclusions of the fifth section	275
References in Chapter 5	277
CONCLUSIONS	282

List of Conditions

2FA	– multi-factor authentication
ABS	– automated banking system
ACCS	– asymmetric crypto-code systems
AGBCEC	– algebra-geometric block code on elliptic curves
AIPSB	– automated information processing system of the bank
BCP	– Business Continuity Planning
BI (BIn)	– banking information
BIA	– Business Impact Analysis
BIT	– banking information technology
BS	– banking sector
BSC	– block symmetric cipher
CCIS	– critical cybernetic infrastructure of the system
CD	– ciphertext of damage
CFT / CHFT	– ciphertext of the flawed text
CI	– critical infrastructure
CIA	– critical infrastructure applications
CIO	– critically important object
CS	– cyber security
CybA	– cyberattack
DAM	– damage
DCH / DCH	– damage of ciphertext
DRP	– Disaster Recovery Planning
EC	– elliptic codes
FT	– flawed text
FTC/FTCH	– flawed ciphertext
HCCDMC	– hybrid cipher-code designs on loss-making codes
IC	– information conflict
IISS	– integrated information security system
IP	– information protection
IR	– information resource
IS	– information security
ISS	– information security system

MACCS	– modified asymmetric crypto-code systems
MAO	– Maximum Allowable Outage
MCIS	– the metasystem of critical infrastructure of the state
MEC	– modified elliptic codes
MIP	– method of information protection
MTPD	– Maximum Tolerable Period of Disruption
NA	– unauthorized access
NSMEP	– national system of mass electronic payments
OBS	– organization of the banking sector
OCCI	– an object with a critical cybernetic infrastructure
PDCA	– Plan-Do-Check-Act
RPO	– Recovery Point Objective
RTO	– Recovery Time Objective
SCCI	– system with critical cybernetic infrastructure
SDO	– Service Delivery Objective
SI	– security of information
SS	– system of detection of attacks
TCS	– theoretical code schemes
The NBU	– National Bank of Ukraine
TMIP	– technical means of information protection

INTRODUCTION

Topicality. In modern conditions, as practice has shown, the important role in ensuring the national security of Ukraine, and especially its economic component, belongs to the processes of ensuring information security of the state in the banking sector (BNC). A key and system-forming role in the process of building a system for providing bank information (BIn) as a component of national information resources of the state is played by theory and practice, in which the scientific and methodological base is the basis for making informed and effective management decisions by the entities providing state budget at all levels. The revolutionary changes of the last decade in the banking sector have led to the unification of information and computer networks into a single information and cybernetic space, which has led to the creation of automated banking systems that have substantially expanded the spectrum of electronic services of state and commercial banks of the world and Ukraine. As a result, threats to such a national information resource of the state as BIn were significantly transformed. Threats have gained signs of hybridization. From purely threats to information security (IS), cyber security (CS) and security of information (SI) manifestations of hybridization of these threats began to occur due to the simultaneous impact on the object of protection — BIn in automated banking systems (ABS) due to the emergence of a synergistic phenomenon. As the global experience shows, for example, such threats were manifested in blocking the work of the ABS BNS in the United States (September 2011), which led to a massive disobedience action called “Take the Wall Street” which, as a chain reaction, spread to the largest cities of the aforementioned state and a number of the most economically developed countries of the European Union, and as a result provoked a world economic collapse.

Manifestations of hybrid threats to the security of BIn in ABS took place in Ukraine. For example, starting with cyberattack with the help of malicious software “Petya. A”, “Petya. B” (June – July 2017), the process of providing banking services was compromised, which provoked dissatisfaction with clients of banks — citizens who are subjects IB state. Chain reaction after Ukraine spread to banking sectors of Italy, Israel, Serbia, Romania, Hungary, Argentina, Czech Republic, Germany, and others developed countries of the world. Thus, the problem of ensuring the state’s IT for critical infrastructure (CI), which includes the banking sector, is very acute. Consequently, it becomes clear that there is a need for a radical overhaul of the current methodological principles for building a system for providing IB BIn in the ABS both in Ukraine as a

whole and in the world in particular. Therefore, work in this direction has been conducted over the last 30 years.

It is known that the problem of solving the problem of the state budget in general and the IB BIN ABS in particular is devoted to the work of famous domestic and foreign scientists and their scientific schools: V. Buryachka, S. Burchyk, I. Gorbenko, R. Grischuk, V. Dudikevich, V. Zadiraki, O. Korchenko, O. Kuznetsova, V. Lakhna, S. Lenkova, O. Moldovian, V. Mohor, A. Novikova, O. Petrova, O. Potia, V. Sidelnikova, O. Stasyuk, S. Timofeev, V. Khoroshka, O. Yudina, M. Shelest, B. Schneier, V. Shokala, V. Yarochnikina and many others. At the same time, it has been established that the problem of creating a holistic, scientifically sound methodology for building a system of providing IB BIN in ABS is an unresolved part of the overall problem of providing state-owned information systems, the introduction of which in practice will contribute to the stable and stable development of the banking sector of the state.

CHAPTER 1. State of the art analysis

1.1 Review of the literature on problem

1.1.1 Analysis of the nature and content of information security problems in the current development of science and technology

The development of society in the early twenty-first century is characterized, above all, the transition from an information society to a society of high technology, providing oversaturation of new information and communication technologies, further development of globalization in the modern economy, the dynamics of information such areas of society as the sphere of communication, energy, transport, system production and storage of oil and gas, financial and banking systems, defense and national security agencies ensure stable operation of central executive bodies, widespread transition to e-governance methods and document [1, 2, 3]. Secondly, information processes throughout the world highlight the important task of information security. This is of special significance for the state of its information resources, increase the value of information in the market, its high vulnerability and often substantial losses as a result of the unauthorized use [1, 2, 3, 4, 5, 6, 7]. On the third place, the rapid development of the Internet and other information and communication technologies shaping the global information space to create new threats and new forms of international conflicts, including information warfare, network confrontation, hackers, etc. The development of computer technology and information and telecommunication networks provide great opportunities to society, while at the same time and generate a new kind of crime — cybercrime [4, 6].

In 2015 a terrorist organization “Islamic State of Iraq and Greater Syria” (ISIS) acquired a unit engaged in conduct computer attacks. In this section of the Internet known as Cyber Caliphate, whose main objectives are evil and disclosure of confidential information, attacks on Internet resources, which include sites of banks, research centers, public enterprises and others [8]. On the degree of danger to society of electronic crimes can be seen along the cost of the remedies that are considered acceptable and appropriate. According to experts of the security of electronic document US, the total cost to protect bank or other financial institutions could reach only about 510 thousand dollars. However, deemed reliable security system of a large financial institution, which serves up to 80,000 clients worth at least \$ 15 million, and this amount includes only the cost of hardware and software (excluding the salaries of state employees own security company) [7].

Information threats can manifest itself in different forms. Cyberterrorism is characterized by the desire for significant destabilization of public order. This phenomenon is closely linked to the development of information infrastructure, with constant growth of society depends on smooth functioning computer systems action aimed at their destruction, causing more significant damage and cause a serious public outcry [7]. This means the targeted cyberterrorism at intimidating the population and authorities, and actual or potential proclaimed (claimed) effects on cybernetic society, socio-technical and technical systems, the commission of which leads to (create conditions for occurrence) danger for the citizens, society and state [1]. On particular concern in the last decade is the use of terrorism to carry out terrorist activities of existing information resources, primarily the Internet. Global Network attracts terrorist groups following the features [1, 6, 9]:

- speed, efficiency and availability;
- weak or no censorship of any kind of control by the state;
- the presence of a huge potential audience members scattered throughout the world;
- fast and relatively cheap dissemination specially matched information, the complexity of its submission and acceptance (sending emails, organization news group, website for the exchange of ideas, posting information on separate pages or in electronic versions of periodicals and network broadcasting and others);
- most servers, communication networks allow users to respect confidential and anonymous;
- it is possible to use special robots (bots) to reduce the time and cost of terrorist activities;
- high efficiency effects that can have both local and global in nature;
- cybercrime is difficult to track and collect evidence;
- the uncertainty of place, time and the process of preparing to implement cybercrime;
- possibility of cybercrime acts simultaneously on different objects or subjects from different directions without the need for any violation of borders;
- the possibility of unauthorized connection to computer networks, management of strategic targets, including military;
- a high degree of anonymity when making cyberterrorism;
- spatial and temporal distance from the object or subject of cyber attacks. All cyberspace influences made directly through cyberspace. Main cyber assets shown in Fig. 1.1.

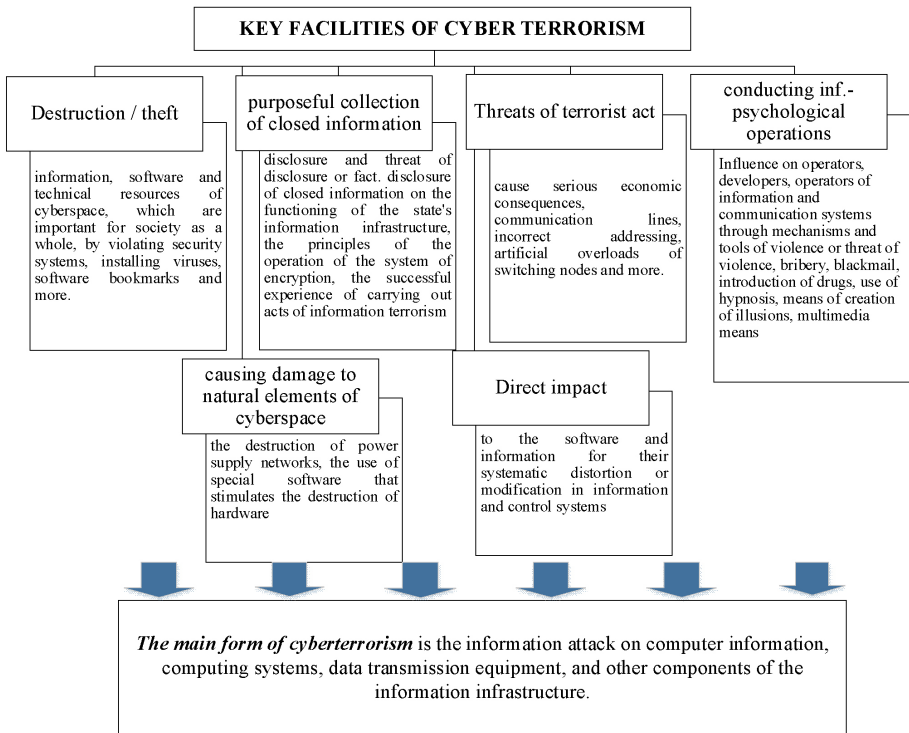


Fig. 1.1. Main assets cyber on the Internet

Analysis of Fig. 1.1 shows that terrorism is increasingly becoming information technology of special type, because terrorists are increasingly using the possibilities of modern information and telecommunication systems for communication and information gathering, most terrorist attacks are designed not only causing material damage and threat to life and people health, but also for information and psychological shock whose impact on large numbers of people creates a favorable environment for terrorists achieve their goals.

Thus, in terms of capacity in the world of globalization and the information society terrorism began to act as an independent factor that could threaten the integrity of the state and destabilize the international situation.

Terrorist groups are increasingly use possibilities of new information technologies and the Internet to spread advocacy and information sharing, attract new mercenaries, collect funds for their support, planning attacks, and for monitoring their conduct [9].

The main uses of new information technologies and the Internet for terrorist purposes shown in Fig. 1.2.

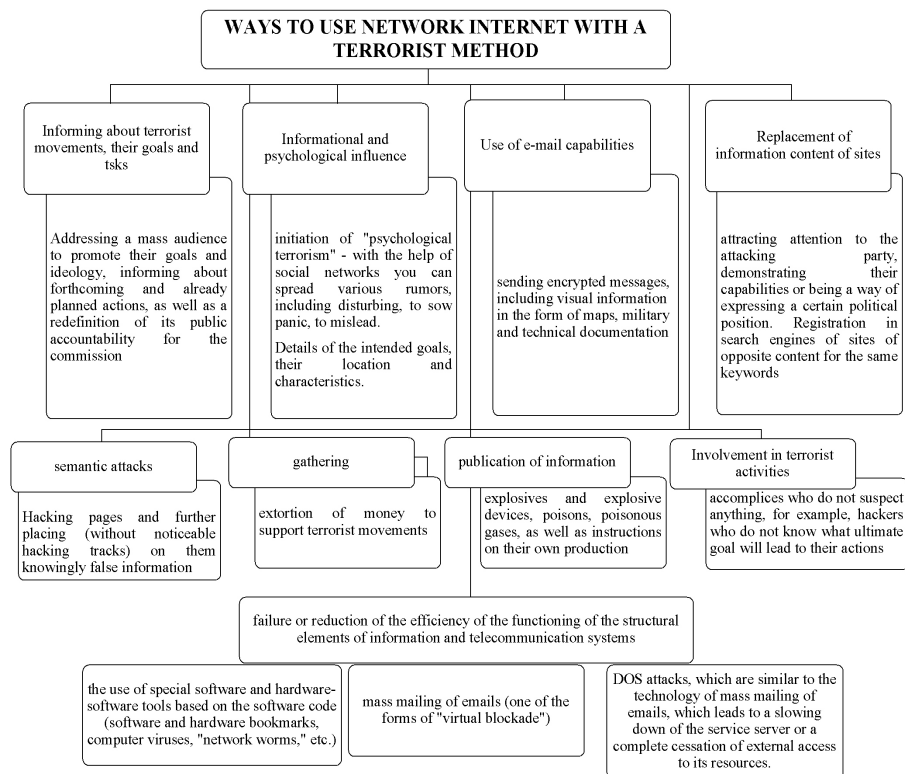


Fig. 1.2. The main uses of new information technologies and the Internet for terrorist purposes

The analysis of Fig. 1.2 shows that social networks are actively used to promote a comfortable life demonstration of the alleged militants, military life and heroism of fighters call to fight for their ideals with arms, broadcast scenes of successful military operations and acts of intimidation. Photo and video reports accompanied by jihadist songs which occupy an important place in the cultural matrix formed global terrorist community. They have their own mobile application and online store where you can buy a shirt or hoodie logo terrorists. All these products dangerous for consciousness extends to many languages.

Active use of cyberspace ISIS in Europe showed the following picture [9]: 84 % — young people come to the ranks of terrorist organizations via the Internet; 47 % — drew attention to the materials (video, text) are online; 41 % — pledging allegiance ISIS online; 19 % — used the online instructions when preparing the attack (making improvised explosive devices and bombs). The main objective of such products — attract and engage stakeholders, involve them in

dialogue in question and answer format for the purpose of psychological treatment for further isolation of man from the inner circle and society as a whole and attracting the ranks of terrorists.

Thus, unlike conventional terrorism, which does not threaten society and as such did not touch the foundations of his life, a modern high-tech terrorism could produce a systemic crisis in every country with a highly developed infrastructure. The development of social networks accompanied by increasing use of their capacity to carry information confrontation, increase coordination, scale and complexity of actions of its members, as are often act as a state, and some organized groups which includes terrorism. The object of cyber-attacks are increasingly becoming information resources, disabling or “difficult position” function, which can cause side opposed to significant economic losses or cause great public interest [9].

Changing security vector world leaders of developed countries towards ensuring cyber security of critical facilities cybernetic structure (CFCS) adopting strategies and concepts with world leading cyber nations, creating national Computer Emergency Response Team (CERT) significantly changed in recent decades, the views of the leading countries on the development of the phenomenon of cyber security and shows that the interpretation given category is constantly evolving. In the evolution of attitudes, significantly affect the level of economic development, the level of education of its population level of the high technology, access to the Internet, etc. The analysis of the basic principles and methods of implementation of cyber threats can be concluded that in the next one to two years, dramatically increase the number and “quality” of cyber threats to CFCS state, allowing the inside to undermine the economic basis of the state metasytem [1, 12, 19, 20, 21, 22, 23, 25, 26, 34, 35, 36].

The analysis of the main provisions of the critical cybernetic structure in [1] allows authors proposed the basic concepts associated with the formation of hierarchical structures critical infrastructure meta-system state:

Critical infrastructure (CI) — systems, networks and/or separate objects, purposeful or accidental conclusion down which could potentially lead to irreparable consequences sustainable economic development and political processes in the country, social welfare and health;

Cybernetic system of critical infrastructure (CSCI) — a set of interrelated elements combined into a single unit, correct operation and interaction which significantly affects the cyber security of the state for a certain time interval;

The object of cybernetic critical infrastructure (OCCI) — cyber element CSCI impact that leads to a reduction in its cyber protection against cyber threats.

Table 1.1 showed ratio results in comparison to the state sector CI [1].

Table 1.1 analysis showed that the most developed countries in the world most vulnerable to critical infrastructures include objects belonging to the banking and financial sector, energy and telecommunications.

Feature based on the approach proposed [36] critical infrastructure hierarchical meta-system state is shown in Fig. 1.3. In modern terms, as shown, an important role in ensuring national security of Ukraine and especially its economic component belongs processes of information security state of the banking sector. And system-key role is the construction of a system to ensure information security of banking information (BI), as part of national information resources of the state, plays a theory and practice in which scientific and methodological base is the foundation for sound and efficient management solutions for IS subjects of state at all levels.

This *meta-system during the critical infrastructure of the state (MCIS)* is a system of strategic scale, which is a combination of a large number of different elements combined within a single critical cyber architecture in a single system, which has a synergy and a common emergent property (supplies, function), which differs from the properties of individual elements of the totality [1].

Fig. 1.4 shows the relationship between the main components of information security (IS) state.

The revolutionary changes of the last decade that have occurred in the electronics industry, combining information and communication and computer networks into a single information and cyberspace, creating automated banking systems significantly expanded range of services in the banking sector. As a result, significantly increased range and threats to the national economy. The key and most potentially dangerous of them is compromised or when taking remote control of management processes in ABS.

The consequences of the absence or imperfection security mechanisms of ABS can have a huge and irreversible, leading eventually to the collapse of the financial and banking system of Ukraine, and economic collapse in the country as a whole.

Analysis of Fig. 1.3 and 1.4 shows that for IS entirely dependent on the state for IS of its components that relate to objects and MCIS affect not only the state of the information security of the state, as well as other components of society and the state as a whole. Threats have become signs of hybridity, so they must be considered as complexing threats that have synergistic effect of all components on the security of the state, IS, CB, SI. Proof of this approach is the final guidance document NBU that adopt "Statement on measures to ensure information security in the banking system of Ukraine" [34] Basic provisions and their relationship shown in Fig. 1.5.

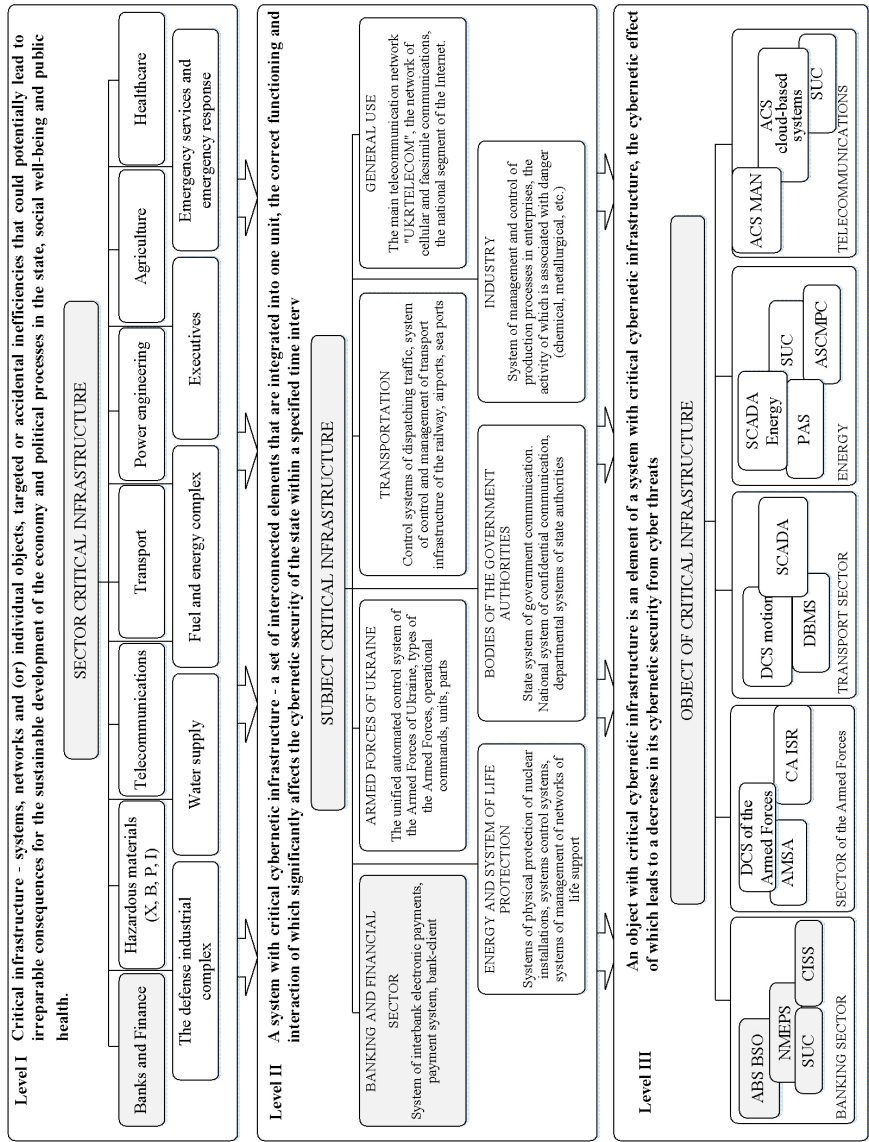


Fig. 1.3. The hierarchical structure of critical infrastructure meta-system state

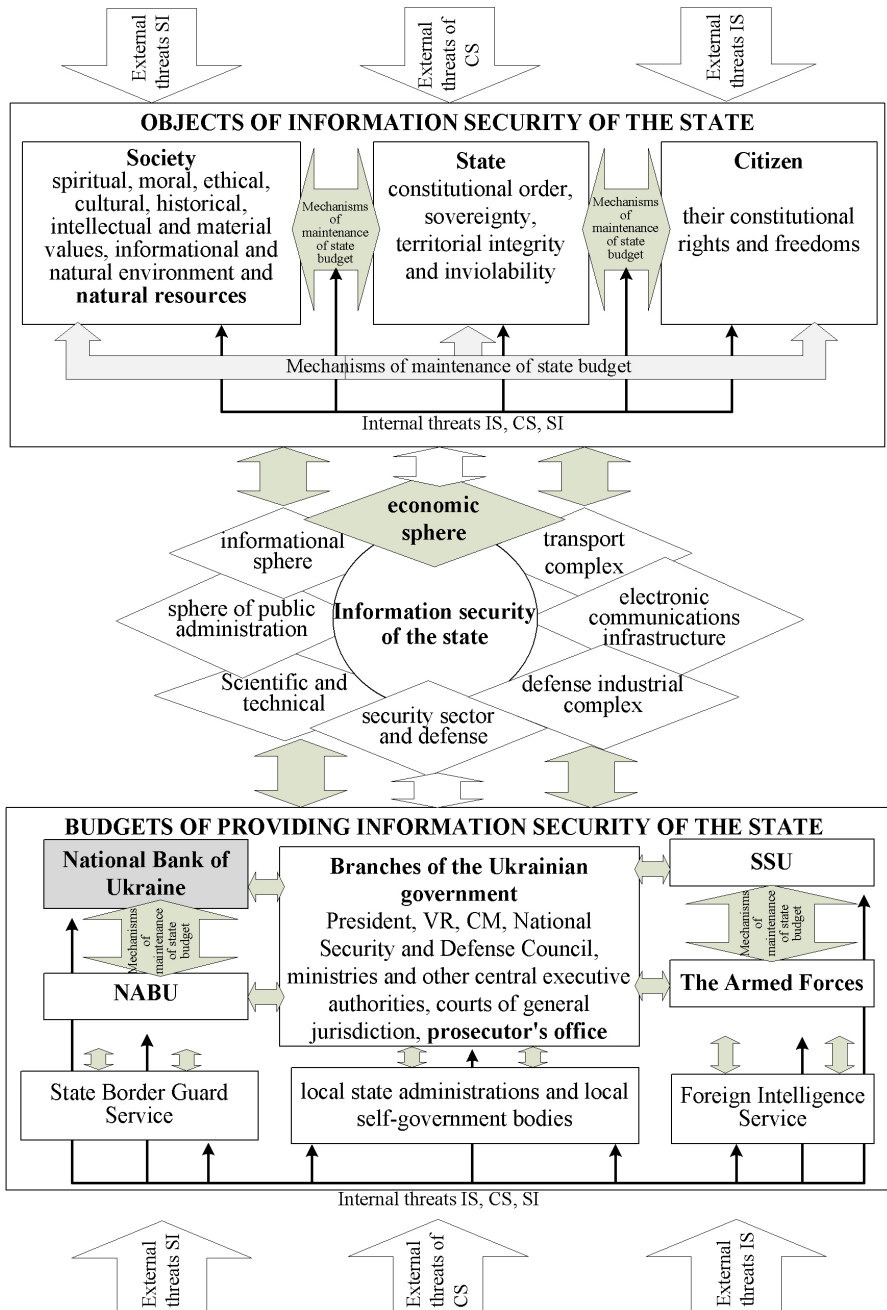


Fig. 1.4. The relationship of the main components of information security

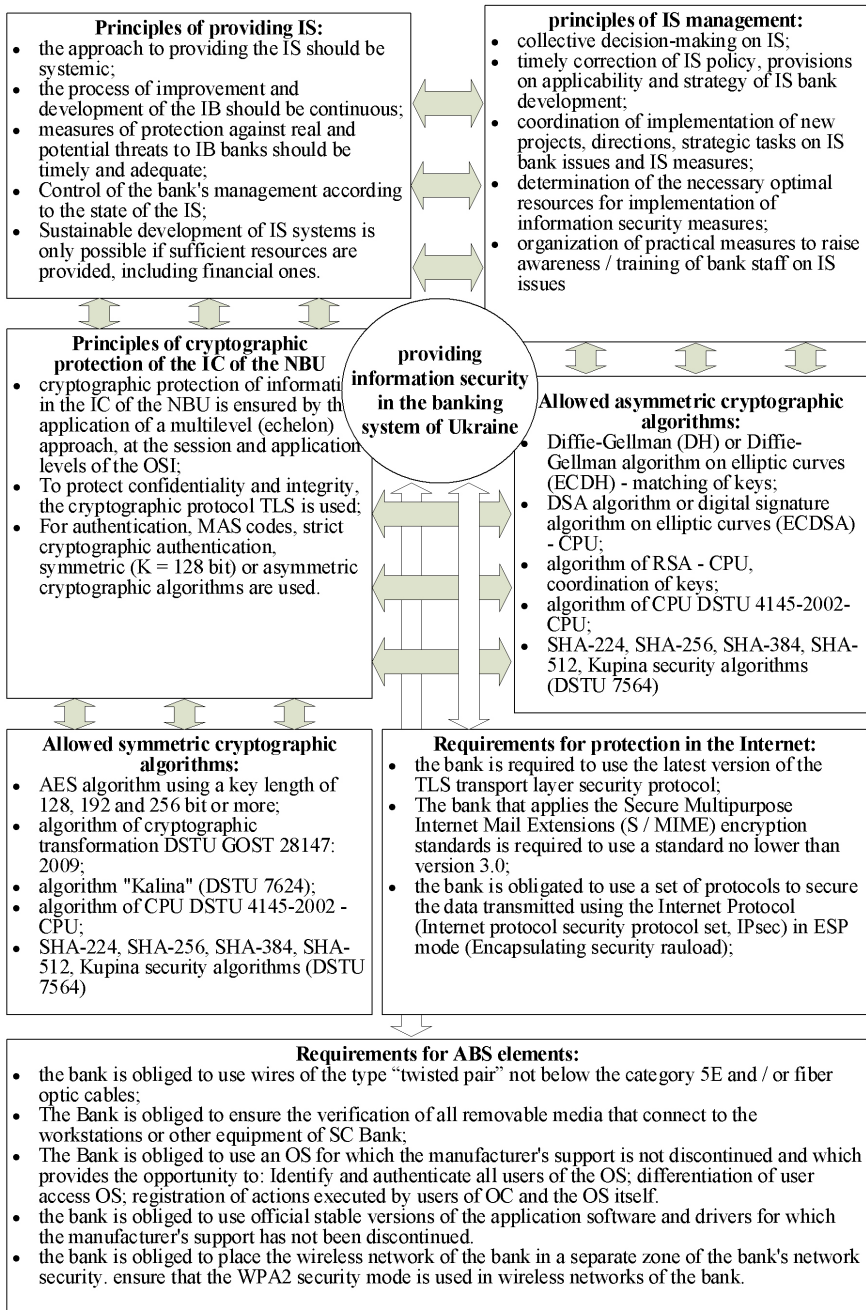


Fig. 1.5. Basic principles and mechanisms for IS OBS in Ukraine

Therefore, to address the whole range of issues related to ensuring cyber security, information security must be addressed in the ABS together and inseparably from each other harmoniously complementing and filling, if necessary, to one another. Easy integration of capabilities in each case to ensure the safety of ABS is impractical, both practical and scientific viewpoints.

Lack other alternative approaches prompts the urgency of solving the problem that has arisen — improving information security in Ukraine based on the ABS new unknown to this day approaches.

It is known that computer and telecommunications systems provide the reliability of the vast number of information systems for various purposes, including banking. Most of these systems carry undisclosed information that is confidential. Thus, the solution of automation of data resulted in the generation of new problem — the problem of information security [37, 55, 56, 57, 58, 59, 60, 25, 20, 21, 19].

From the time of its introduction, banks invariably caused criminal interest. And this interest was associated not only with the storage of credit organizations of money, but that banks often concentrated important and secret information about financial and economic activities of many people, companies, organizations and even entire nations.

Thus, regardless of the means, mechanisms and technologies to ensure security of banking information by another pressing problem, and the second total score is the problem of information security of individuals, society and the state in which man — a bank employee or customer — the most vulnerable link [33, 39, 40, 41, 42, 29].

Computerization of banking activities has significantly increase the productivity of bank employees, introduce new technologies in financial products. Internet banking is now widely spread among banks and clients use Internet resources as an alternative means of transmission of PIN client bank not only leads to lower transfer costs, but also helps to improve the bank's competitiveness, increase the flexibility of the bank's customers. The main obstacle to Internet banking is the issue of cyber security, and the lack of trust and legal support [42].

As an example of note is the fact that 90 % of all crimes in the banking sector — a cybercrime associated with the use of automated data processing bank systems (ADPBS) [38]. Therefore, the protection of its own banking system should use powerful authentication and control actions, both internal users and customers. It is generally accepted that the most reliable means of protection can provide two-factor authentication, whether electronic keys (tokens) or one-time password generators [46, 64, 65, 66, 67]. Data security

during storage requires the use of encryption, which can operate at storage, or at the individual system components, such as database tables. Safety ATMs and payment terminals must be provided with the use of anti-virus protection. But at the same time, the specifics of such devices requires the use of additional security arrangements, including the creation of “closed software and hardware environment”, eliminates the installation of any third-party software and external devices [17, 18, 29, 33, 34, 39, 41, 44]. Thus, the problem of cyber security as an integral part of the third on the way to solving the problem of security banking information [45, 46, 47, 48].

To ensure adequate security system banking information no matter what part of it is the problem of information security, information security problem or the problem of cybersecurity, as appropriate to apply the principles of risk management methods [40]. This method with the right approach will allow time to identify and classify threats and the likelihood of adverse consequences of their possible manifestations organize a system of adequate security banking information. But given the imperfect method principles of risk management in the banking sector still requires the necessary proof raised in the context of the above problems.

In work [29] noted that security information including banking can be provided only in the complex of available remedies in all structural elements of the production system and at all stages of the processing cycle of information. This approach is the basis for IS banking institutions NBU [34].

Ignoring system analysis methodology to establish system of banking information based on the difficulty and sometimes impossibility of objective confirmation of established system efficiency due to imperfect regulatory and methodological information security, especially in the field of indicators and criteria [41] just creates obstacles to the solution of the abovementioned problems. For example, the international standard for transactions on bank cards with chip (EMV), introduced in 2005, defines the physical, electronic and information interaction between credit card and payment terminal for financial transactions based on standards ISO/IEC 7816 for contact cards and ISO/IEC 14443 for contactless cards.

Thus, from the study of literature, we can conclude that a fundamentally new effect in securing bank information can be achieved if and only if all the above means, methods, measures and safety technology combined in a single integrated mechanism hereinafter called synergistic.

1.1.2 Investigation of the role and place of information security system of banking information in automated banking systems

Given the rapid development of science and technology over the past decade, and intensive use of the latest high-tech developments in the banking sector nature and content category “Banking Information” changed significantly. Today, as you know, the banking information is based on the components of modern ABS. Based on this and building on [43, 61] can be argued that under the bank account in the broadest sense refers to a set of data associated with registered documents and guidance of banking institutions, the legal form of banking institutions, current form banking institution and its employees, types and forms of banking, quantity and composition customer transactions on customer accounts, the presence of correspondent relations and technical support of the bank. Given the breadth of categories, embraces banking information with a view to its correct application feature classification proposed banking information (Fig. 1.6).

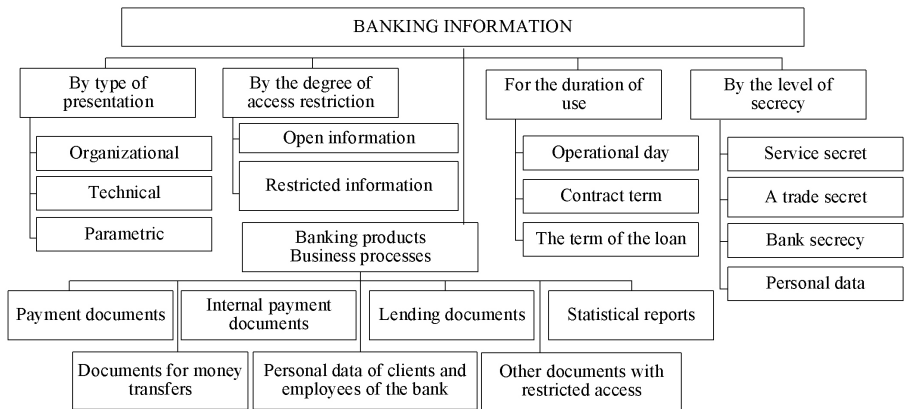


Fig. 1.6. Feature classification of banking information

The advantage of the proposed banking information feature classification (Fig. 1.6) is that it is unlike the known classifications reveal the depth of the content essence of this category. For example, types of banking information is organizational, technological and parametric. Thus, under the organizational bank account information should be understood that reflects the nature of business relationships with bank customers about features of organization and construction management of the bank.

Technology banking information — is an information on the principles of the bank in carrying out all kinds of banking activities and information systems used in bank protection latest high-tech developments. Parametric banking

information — information that reflects quantitative indicators, reflecting the bank capital and the value of its loan portfolio the bank in the implementation of all activities. Another advantage of the proposed classification is that in case of new features that characterize the various aspects of banking information category in the proposed classification provides the ability to expand the set of features.

With the proposed classification, also conclude that in the subsystems ABS Bank circulates information at different levels of confidentiality (privacy) of open information to the data containing classified information (commercial, banking and official secret). In the ABS Bank documents also present: money orders and other cash and cash documents, reports (financial, analytical and other) data on personal accounts, general information and other confidential (restricted distribution) documents, etc., can also be referred to the concept of banking information.

Thus, in the most general terms during bank account can understand the information arising from banking activities. This is particularly the information characterizing the bank itself, its financial position, performance and reliability requirements of the law. This information can be gleaned from the Bank's Charter, its licenses, balance sheets, statements of income and other sources. In addition, in a narrower sense banking information — is information about specific operations of the bank. This information describes not only the bank, but those which the bank enters into a relationship. As an example, banking information can give information about the presence of deposits or accounts and transactions on them, on the property, which is deposited in the bank.

Whether in a broad or narrow sense treated meaningful categories of banking information activities of all the subsystems of ABS in which it is produced, processed, stored and circulated provided and regulated through laws and recommendations of the National Bank of Ukraine. Therefore all major existing regulations governing the processes described above at the national level in a systematic form can be presented as a block diagram (Fig. 1.7).

A critical analysis of the current legislative framework of Ukraine showed that to protect information in the ASS used by information security management system (ISMS) to control the operation of complex information security systems. Thus, according to the preliminary conclusion of ABS is an integrated information banking system that integrates different areas of the bank, able to automate and combine into a single purpose business processes of financial institutions. Integrated system supporting centralized processing, multi-currency and automation of key financial transactions should ensure the effective management, control, receiving reports about the current activities of all branches of the bank [9, 31].

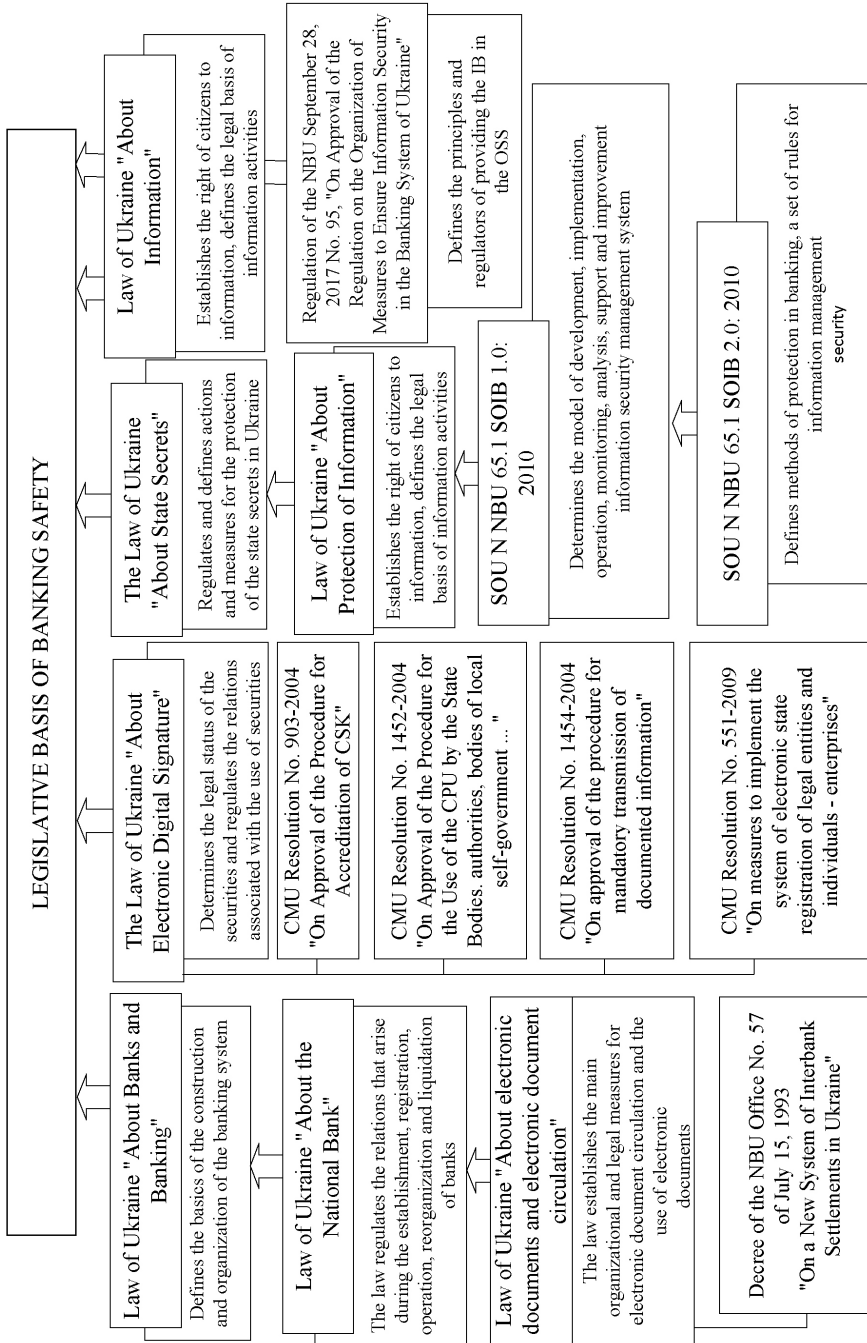


Fig. 1.7. The current regulatory framework of the ABS in Ukraine and its relationship

Among the functions inherent in modern integrated ABS, the following: working day; transactions on the stock market of the Bank's securities; farm activities; retail banking; remote banking services; electronic banking services; payment center and the payment system (card products); integration of back-office bank with its external operations; management of the bank's business logic implementation, monitoring, accounting, including tax and reporting; risk management and strategic planning; customer loyalty programs, marketing, advertising and PR-service.

As known [23, 24, 26, 28, 29, 34, 37, 38, 39, 40, 41, 42, 43, 56, 57, 58, 59, 60, 61] main functions of the ABS are realized through the use of the following technology and banking information security:

- database management system (distributed databases);
- data storage, OLAP- OLTP- and data processing technology (online analytical processing system and operational transaction processing system);
- search engine extraction and preparation of reliable data;
- distributed computing system, the organization of collective users create real bank information space, including branch offices, customers and partners;
- secure connection of the information system of the bank to external computer networks (the Internet);
- organization of safe, reliable public data communication channels (cryptography, encryption and digital signature (DS), arrangements), electronic document;
- technical, software, mathematical and other support;
- Information Analysis and decision support systems (decision support systems, DSS);
- protection of information stored and processed, the entire ABS in general;
- system remote work with stock markets and behavior prediction software courses;
- CRM-systems, customer relationship management;
- program of the front-office customer interaction;
- support system of internal organization, management and executive staff activities;
- access to information of different levels of secrecy;
- virus protection;
- online shopping and online card;
- call centers and IP- telephony;

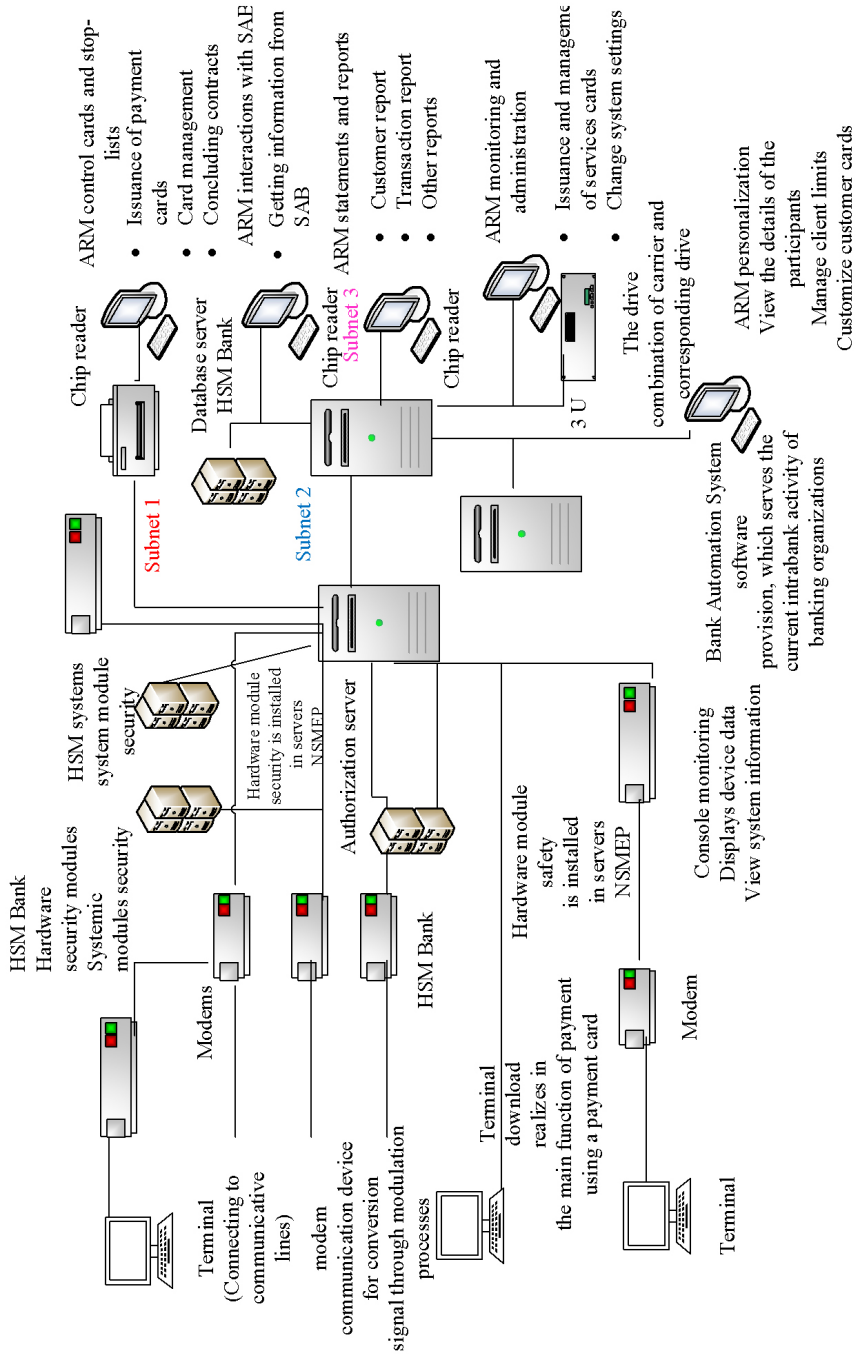


Fig. 1.8. Block diagram of the ABS NMEPS

- support various access channels: Internet, telephone, mobile web, SMS, WAP, etc.;
- support for multiple accounting standards including management accounting;
- support and research in the field of systematic information ABS.

ABS NMEPS example shown in Fig. 1.8.

The analysis of the organizational structure NMEPS showed that underlying performance of the functions of its work using automated card system (ACS) — software and hardware with which enforced functions member (s) or member (s) NMEPS on card issuance, processing information on operations with their application, control terminals and ATMs, etc. This system applies to complex multilevel control systems of critical application (CSCA), which requires transmission of information security controls at every level [64].

The system is integrated into the banking system and the many types of terminals, including portable working offline, and ATMs that perform a wide range of functions. NMEPS controls the flow of electronic money, communications terminals and local area networks. To ensure reliable operation of the electronic payment system must be protected.

In terms of information security in NMEPS there are vulnerabilities: sending payment and other messages between banks and customers and between banks; processing information within organizations and destination of messages; customers to access funds accumulated in the accounts.

1.1.3 Research infrastructure facilities threats automated banking systems

The revolutionary changes of the last decades that have taken place in the banking sector led to the unification of information and computer networks into a single information and cyberspace, which led to the creation of automated banking systems, which significantly expanded the range of electronic services to government and commercial banks in the world and Ukraine. As a result, substantially transformed and threats that the national information resource states like BI. Threats have become signs of hybridity. From a purely threats to information security, cyber security (CS) and security of information (SI) displays signs of hybridity these threats began to occur as a result of simultaneous action on the object of protection — BI in automated banking systems (ABS) due to the emergence of synergy effects. As international experience shows, for example, displays such threats have occurred during blocking of ABS BNS in the US (September 2011), which resulted in the emergence of mass actions of disobedience called “Occupy Wall Stritt” which is like a chain reaction spread to largest city of the state and mentioned some of the most

economically developed countries of the European Union and as a result provoked a global economic collapse.

Manifestations of hybrid security threats BI in ABS occurred in Ukraine. For example, beginning with cyber attacks using malicious software “Petya. A”, “Petya. B” (June – July, 2017) has been compromised by the provision of banking services, the bank customer dissatisfaction triggered — citizens who are subjects IS state. Chain reaction after Ukraine has spread to the banking sector in Italy, Israel, Serbia, Romania, Hungary, Argentina, Czech Republic, Germany and others developed countries. Thus, the problem of information security critical infrastructure usage (CIU), which include the banking sector and is very serious. Thus, it is clear that the need of radical revision of existing methodological framework for designing systems for IS BI ABS in Ukraine as a whole, and in particular the world. To find the necessary and sufficient conditions for achieving synergies security of public and private banking systems protect, analyze and specify the set of actual security threats banking information. But before proceeding to solve private problems outlined above, we note that for the first time based security of banking information offered to put the principles of synergy. At the same time interacting profiles that provide banking information security should be considered IS, CS and SI BI, which until now were considered either separately or in combination, that are not allowed to receive a synergistic effect in securing bank information. After decomposition of some security profiles examine them separately to determine the most pressing threats. Based on [44] hereinafter compromise the bank will understand random or targeted, potential or real action of a different nature, which can inflict damage to the bank.

It is known that for the analysis of the main types of threats to information security of banking information model can be adapted triad CIA (confidentiality, integrity, availability) [38, 56]. The model under banking safety information should understand the process of ensuring the confidentiality, integrity and availability of information to customers/customer of the bank based on the totality of collective and individual consciousness. However, under confidentiality refers to access to information only to authorized users, when integrity — ensuring the accuracy and completeness of information and methods of processing to authorized users under accessibility — access to information and associated assets of authorized users as needed.

Given the nature of banking information security threats basic banking information are as follows [64]:

- Violation of privacy: revealing passwords with tacit active network connection, traffic analysis protocols to identify, create false claims to obtain payment documents, unauthorized entry of data, extract statistical information

from the database based on semantic connections between classified and unclassified information, connect to the CS as active transponder (falsification of payment instruments), phishing, pharming, pretexting, screaming, virtual kidnapping, unauthorized transfer of hidden VHF in order to copy data or access to legal CS as a result of secret visit after hours, tacit alteration of equipment or software to implement means of unauthorized access to information;

- Violation of integrity: copying data from magnetic media left on tables or computers, copying data from equipment and magnetic media, harvested in a special storage, usage included in the terminal, left unattended copying and theft of software, changes to data and programs forgery and falsification of financial documents as a result of secret visit after hours, picks up data from hard and floppy disks, changes to the data recorded on left unattended magnetic media, software use for protective capacity of the system, unauthorized use of computer resources, destruction of equipment, magnetic media, or remote data destruction, modification or reading information in a database or individual files after conferring with foreign powers to modify financial information, the substitution of items of equipment left unattended during business hours;

- Violation availability (authentication): unauthorized use of information, a high level of privacy, unauthorized abuse of authority for access to bypass security mechanisms, denial subscriber of the fact of reception (transmission) or create false information about the reception (transfer) messages for the removal of responsibility for the execution of these operations, the penetration of the system through CS communication by assigning authority for the purpose of fraud, theft or copying of information, abuse of privileges supervisor in violation of the protection mechanisms banking, formation, revealing passwords with kidnapping or visual observation, directly or disclosure of the data.

Among the threats to information security of banking information affecting the bank, the bank staff and its clients, as well as the economic component of national security is internal and external threats. As the first and second in focus and the impact on the activity of certain subjects and objects may be economic, physical and intellectual [25, 60].

Economic threat: Corruption, fraud, unfair competition, the use of inefficient banks banking technology production. Implementation of such threats lead to damage to their banks or omissions benefit.

Physical threats: Theft, looting property and funds of banks failure, disabling equipment banks, inefficient operation capabilities. As a result of these threats damages cause banks losses associated with the loss of their property and the need to incur additional costs to restore the means of production and other material.

Intelligent threat: Disclosure or misuse bank information, discrediting the bank in the banking market, various social conflicts around banks or themselves. Implications of such threats: losses of banks, their image deterioration, social or psychological tensions over the banks or their teams.

The third essential safety profile banking information offered to consider size. Cybersecurity — a set of tools, policies, principles of safety, security guarantees, risk management approaches, actions, training, insurance and technology used to protect cyber environment, resource organizations and people [48, 49, 59]. According to the standard, ISO/IEC 27032: 2012 Information technology – Security techniques – Guidelines for cybersecurity also rely on the task to ensure the conditions to achieve and preserve security properties of the organization's resources or users against cyber threats relevant. This cyber security covers such a thing as the protection of personal data and interacts with network security, application security, online safety and security of critical information infrastructures (Fig. 1.9).

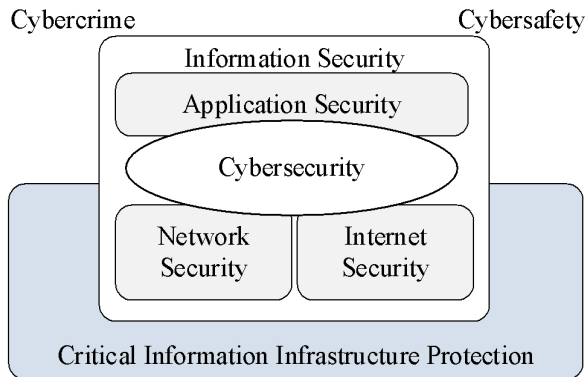


Fig. 1.9. Logical relationships and other cyber security domain in compliance with the ISO/IEC 27032: 2012 Information technology – Security techniques – Guidelines for cybersecurity

Analysis of results in estimates of the number of cyber-attacks, including on ABS, the balance of the complexity of the software and technical literacy criminals received such companies as “Arbor Networks” [62], Cisco [63] and other vendors in the market and cybersecurity means of network peripherals, leads to the conclusion that with the growth of cybercrime and computing capacity in the near future be expected to increase not only the quantity and the technical complexity of cyber-attacks but also on their redirection on peripheral network equipment. With this in mind, and based on the results of studies [1, 3, 6, 12, 22, 29, 34, 38, 40, 41, 57, 58, 59, 62, 63] can be argued that the main

threats to cybersecurity ABS aimed at disrupting the processes of management or taking them under control will cyberattack that can be combined into four major classes of the content of which is disclosed in Fig. 1.10.

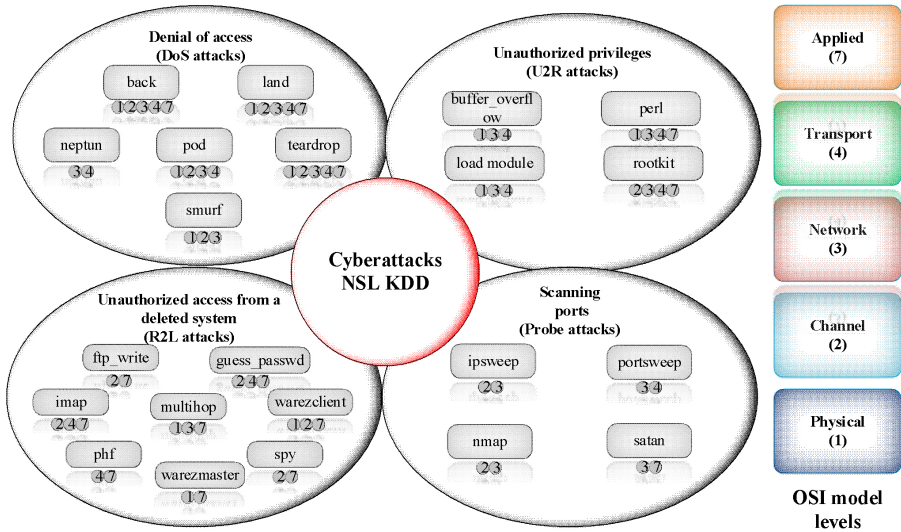


Fig. 1.10. Classification of cyber-attacks on ABS with reference to the OSI model

The classification (Fig. 1.10) clearly shows that different classes of cyber-attacks regardless of functional purpose take place at different levels of model of Open Systems Interconnection OSI, and consequently have their own specific purpose to influence the bank information. For example, before cybercriminals because of the vulnerability of protocols and services the lower level of the OSI model opens opportunities for banking information technology, but because of the vulnerability of protocols and services the upper levels — the organizational and parametric bank information.

Given that the above threats due to various subjective and objective reasons have continue to occur most famous and projected ABS, and building on the close relationship between the different security profiles, and, in order to develop an effective system of protection of banking information, proposes a new model of banking information security threats in the future called synergetic (Fig. 1.11).

The peculiarity of the proposed model (Fig. 1.11) is reflected on it in the form of logical connections interaction of different threats to security profiles. Therefore synergetic model of banking information security threats provides necessary and sufficient conditions for the development of new methodological basis in achieving synergies in the field of security of public and private banking systems of protection.

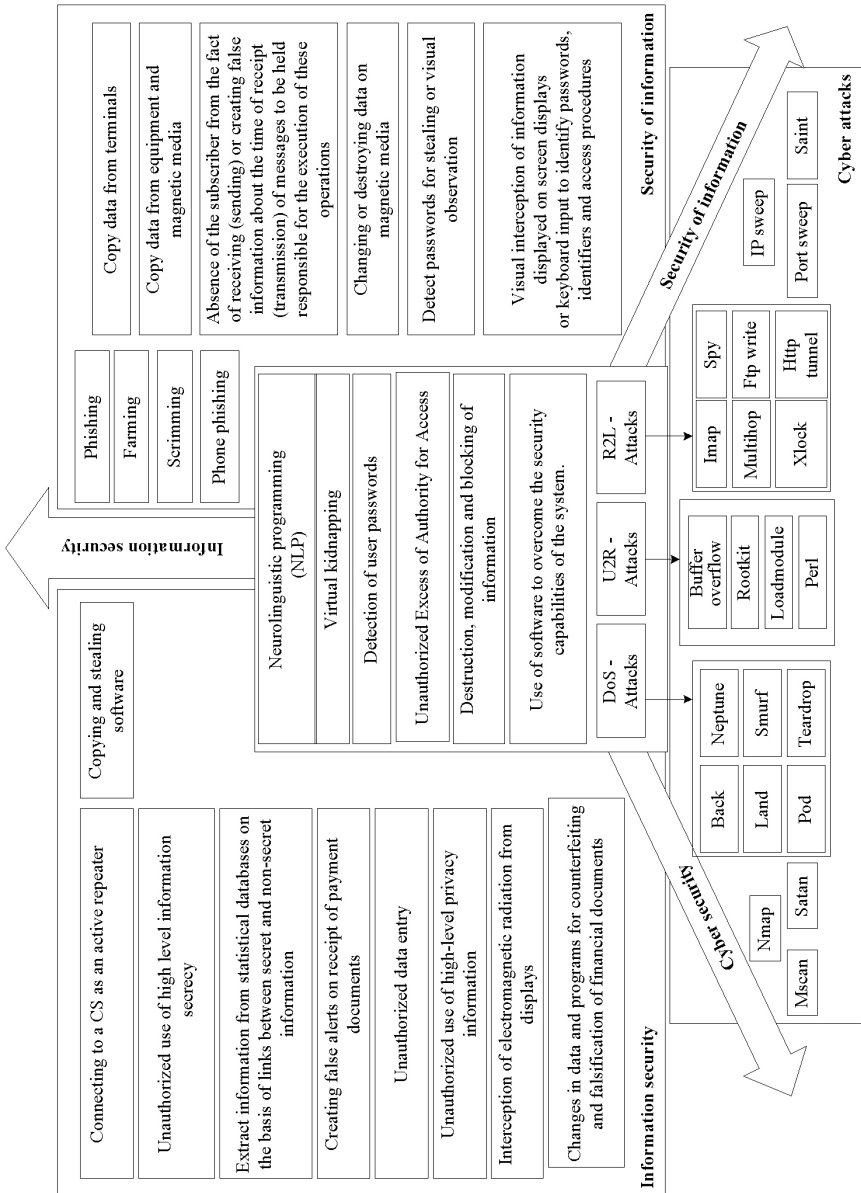


Fig. 1.11. Synergetic model of banking information security threats

Based on a model developed synergistic (see Fig. 1.11) also becomes clear mechanism of nucleation banking information security issues in space-time continuum: the goal of cybercriminals (competitors of cybercriminals, individual states, etc.) are coordinated in time, place, tasks, goals and forms of implementation.

Given the nature of construction means the network periphery [11, 37, 39, 40, 41, 44, 48, 50, 51, 56] and communications organization in ABS any bank synergetic model allows us to establish vulnerabilities in their security system. These are processes associated with sending a payment and other messages between banks (business process/business products) between the bank and ATM, the bank and the client. Features consequently give rise to several problems of systemic nature:

- problems establishing mutual authentication when establishing a connection (mutual recognition subscribers);
- problems of privacy and the integrity of documents (protection of electronic documents transmitted channels);
- problems evidence of the fact of sending and delivery of documents (protection of the exchange of electronic documents);
- problems of mutual distrust between the sender and the recipient through their membership in various organizations and mutual independence (enforcement documents).

An integral part of the problem bank information security is the issue of risk analysis. In fact, the risk is an integral assessment of how well existing remedies able to withstand attacks on banking information.

At present, clearly there are two main groups of methods of evaluation of security risks. In refraction in the banking sector on the basis of the first group may set the level of risk by evaluating the extent to defined set of requirements for the safety of bank information. The second group of techniques of risk assessment reduced to determining the probability of attacks and levels of damage. In this case, the estimated risk value for each attack and, in general, is a product of the probability of an attack by the amount of possible damage from the attack. The value of the loss is measured owned banking information, and the probability of attack is calculated by the panel conducting the audit procedure.

In any social sphere (to which the region and the security BI in ABS OBS) security incidents, disruptions (disruptive events) and accidents (disasters) are inevitable. However, their impact on the company should be minimized, the data should be stored, hardware is operational, reputation rescued people — out of danger [13, 14, 34, 36]. The decision of these problems can take

place within the framework of business continuity management (Business Continuity Management) — a holistic management process, in which the identified potential threats to the organization, evaluated the possible impact on business operations in the case of these threats, as well as a system of regulations to ensure the ability organization to recover its activity and respond effectively to incidents that can guarantee the interests of stakeholders to ensure the protection of reputation, brand and make transactions value, so it is primarily the implementation of the strategy and management cycle is necessary to ensure continuity solving such problems [16].

There are two basic tools of business continuity [13, 14, 15]:

- business continuity plans (Business Continuity Planning, BCP) — a set of preventive measures, detailed instructions for action in acute (critical) situations in OBS further discusses measures to restore BI (Data Recovery BI) provides complete clarity in which they were copied, reflecting what their size, how they should be interpreted otherwise. Determine the maximum “age” data loss is permissible (Recovery Point Objective, RPO);
- Disaster Recovery Planning (Disaster Recovery Planning, DRP) — training organizations to speedily complete restoration of its operations in the event of an accident, emergency, disaster, crisis, etc.

Despite the difference, BCP and DRP are integral parts of business continuity management and procedurally intersect. In this respect it convenient to consider using the model management PDCA (Plan-Do-Check-Act) [13, 17, 18], the main problem on the stage management PDCA model shown in Fig. 1.12.

Thus, the proposed solution has its cost, compatibility, complexity of implementation, deployment time and performance, and can be used both individually and as a set of measures implemented before, during and/or after the incident that caused the discontinuity of functioning ABS and OBS activities.

Assessing the impact of interruptions to business (Business Impact Analysis, BIA) is a key topic of business continuity and consists of a functional analysis of how the interruption will affect the organization. BIA referred to the problem [13, 14, 15, 16] determining the value of each business process; identification and ranking interrupt each business process; prioritization of business processes; resource assessment to ensure business continuity. The final result of the BIA is the choice of business continuity management strategies. In determining the value of business process information systems (ABS) can be fixed at a number of technical indicators [13, 14, 15, 16], the relationship between them is shown in Fig. 1.13.

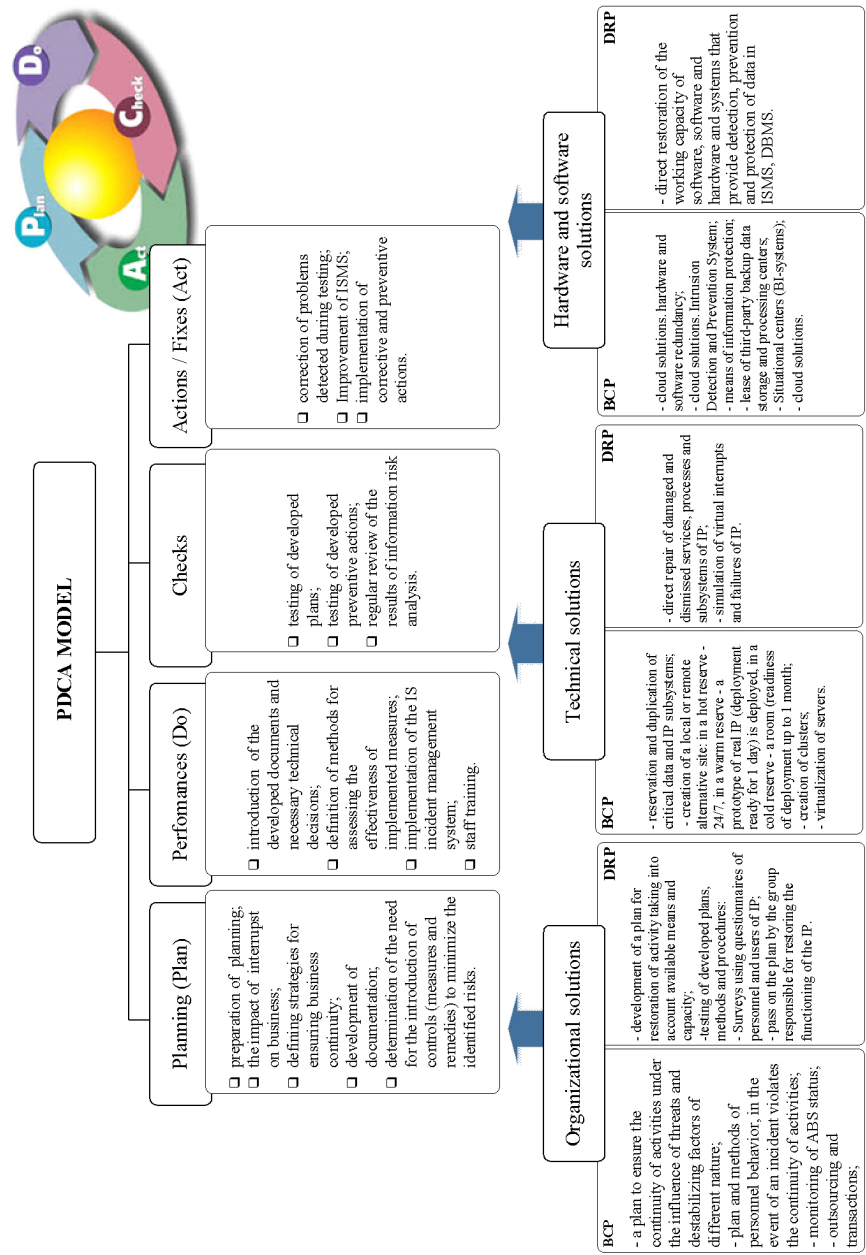


Fig. 1.12. Main tasks and decision stages to ensure continuity management PDCA model

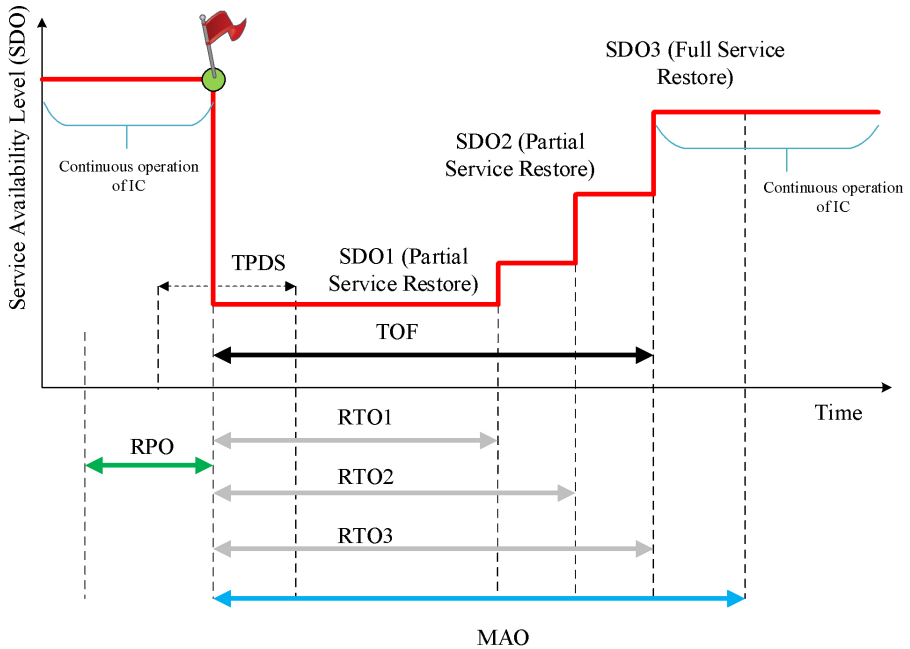


Fig. 1.13. Determining performance business continuity

Key signs:

- MTPD (Maximum Tolerable Period of Disruption, the maximum acceptable period of interruption of business) — the time period after which the adverse effects resulting from the interruption of business, are not eligible;
- RTO (Recovery Time Objective, target recovery time) — the period of time after the event of interruption during which must be renewed a minimum level of the organization and its supporting systems, applications and functions. It is believed that: $RTO < MTPD$;
- RPO (Recovery Point Objective, recovery point objective) — the period of time during which the data must be recovered after the last interruption;
- MAO (Maximum Allowable Outage, maximum idle time) — the time period after which there is a risk of the final termination of OBS, if the provision of services, data, business processes and/or services will not be restored;
- TOF (currently idle) — the period of time during which the activity was interrupted as a result of failure or ABS components, unavailability

of services and data, suitable for enterprise case be less than the maximum allowable downtime. It is believed that $TOF \leq MAO$;

- SDO (Service Delivery Objective, target service availability) — shows the availability of the service at any given time;
- TPDS — planning and deploying solutions to ensure continuity and restoration activities, ideally decisions and plans should be developed and implemented before the incident discontinuity, $TPDS \ll RTO$.

Analysis of Fig. 1.13 shows that reducing TOF requires an integrated approach to solving BCP and DRP. Implementation of preventive measures to protect against cyber threats aimed at the discontinuity will not only minimize data loss BI in ABS, but also reduce the target recovery time.

A similar effect is achieved by the fact that the plans and means of ensuring business continuity are developed and deployed not in the failure, and during the regular functioning of the ABS to implement threat and occurrence of avalanche effect. This allows immediately after the incident to coordinate actions of staff and begin restoration or completely avoid downtime and operational losses by switching to a backup area (Fig. 1.14) [15, 36].

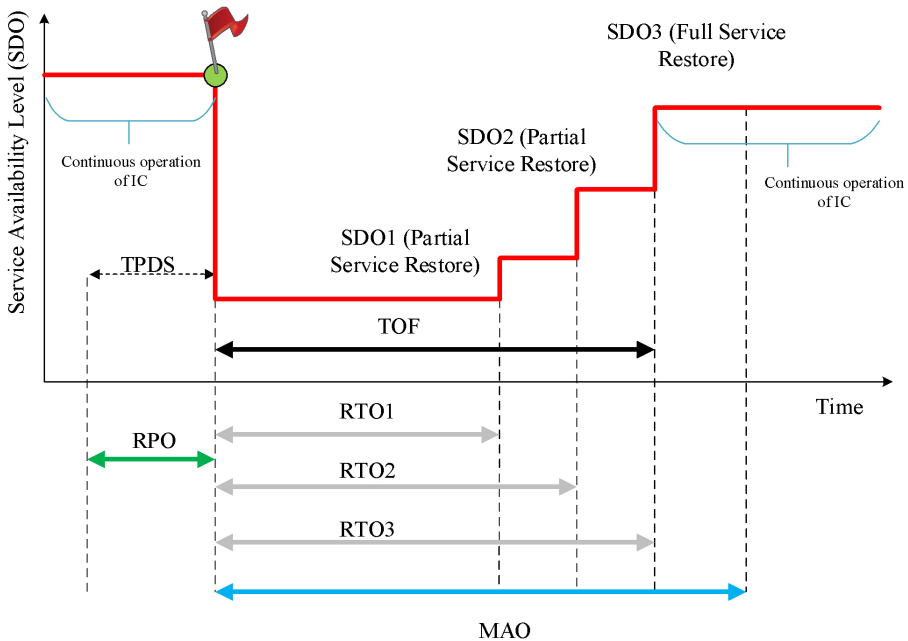


Fig. 1.14. Reduced recovery time operation of the ABS (TOF) through the use of preventive measures and protection plans

Thus, to ensure a comprehensive approach to business continuity OBS proposed to use overlapping the ABS based on the concept of alternative plane (the area in hot standby (Hot Site), the area in warm standby (Warm Site), area in cold reserve (Cold Side) using strategies for updating the data — copying backup data (electronic vaulting, off-site data protection, periodic transfer copies of databases to alternative media, usually in batches), remote logging (remote journaling, log periodic transmission gear made shares a main plane at alternate), remote mirroring (remote mirroring, full duplication in real time), which provides the required performance value of business processes. The proposed approach to ensure business continuity in ABS OBS confirmed in the Resolution of NBU “On approval of organizing the information security in the banking system of Ukraine”.

1.1.4 Analysis of current state services and mechanisms for cryptographic protection of banking information

Protection system of electronic banking documents in a computer network NBU has complex hardware and software encryption and key system to them, technical and organizational measures to protect information online. According to the Concept of electronic money circulation in Ukraine approved by the NBU 02.10.92, designed and manufactured hardware and software cryptographic protection of electronic banking documents in a computer network NBU, in particular:

- protection of bank data (PBD);
- protection of electronic money circulation (PEMC);
- key system with key generation and secure the NBU electronic media keys (codes);
- electronic card (EC).

Protection compliant with GOST 28147–2009 algorithms for encryption and is certified by the State Service of Ukraine for Technical protection of information meets all the requirements of the computer network “Bank”.

Quality solving the above problems is largely determined by rational choice cryptographic tools, implementation of protection mechanisms.

According to international standards ISO 7498, ISO/IEC 10181 to provide the necessary safety parameters generally identified five basic services, the main ones are only two: the authenticity and integrity, to ensure their security mechanisms are used, most of which are implemented based on cryptographic techniques conversion information. The main mechanisms to ensure the integrity and reliability of information in banking systems at different levels based on the use of standards symmetric block cipher (3DES,

GOST 28147–2009). Block diagram of the integrated protection system in the ISMS NMEPS shown in Fig. 1.15.

To ensure maintenance of electronic document circulation in ABS using digital keys (certificates) in accordance with ISO standard ISO/IEC 9594–8: 2006 [68] CISS is an example of DSW “X.509 Code”.

Cryptographic information security “Cipher, X.509” is designed to: create public key infrastructure (creation of DSW, including accredited centers registered under the responsibility of the DSW, to provide users with key management tools).

Provision of electronic services by public authorities, local governments, enterprises, institutions and organizations of any form of property and individuals. CIPF functional purpose “X.509-Code” are:

- management software keys and certificates in accordance with ISO/IEC 9594–8: 2006;
- providing cryptographic protection of confidential and public information, computation and verification of digital signature data according to ISO 4145–2002, encryption and data masking to GOST 28147–89 formation hash functions in accordance with GOST 34.311–95.

CIPF “X.509-Code” is a software package, which means the OS runs on computer technology and interact with the general application software, the general structure shown in Fig. 1.16.

Organization of network interaction between the components of CIPF requires special attention, a typical network topology CIPF “Code-X.509” shown in Fig. 1.17.

CIPF “Code-X.509” supports the following cryptographic algorithms:

- Creating image data is performed using hash function algorithm GOST 34311–95;
- Managing encryption keys provided by the protocol Diffi-Hellman in accordance with paragraph 5.3 and p. 6.1 ISO/IEC 159461–1 (in polynomial basis) and p. 8.2 ISO/IEC 15946–3 (without multiplying a polynomial basis).

It supports all key length recommended standards:

- encrypt, decrypt data and masking performed by the algorithm GOST 28147–89 (GOST 28147–2009);
- formation and electronic check algorithm implemented ISO 4145–2002. It supports all key length recommended standard.

Fig. 1.18 gives the relationship between the mechanisms and standards applicable to ISMS NMEPS.

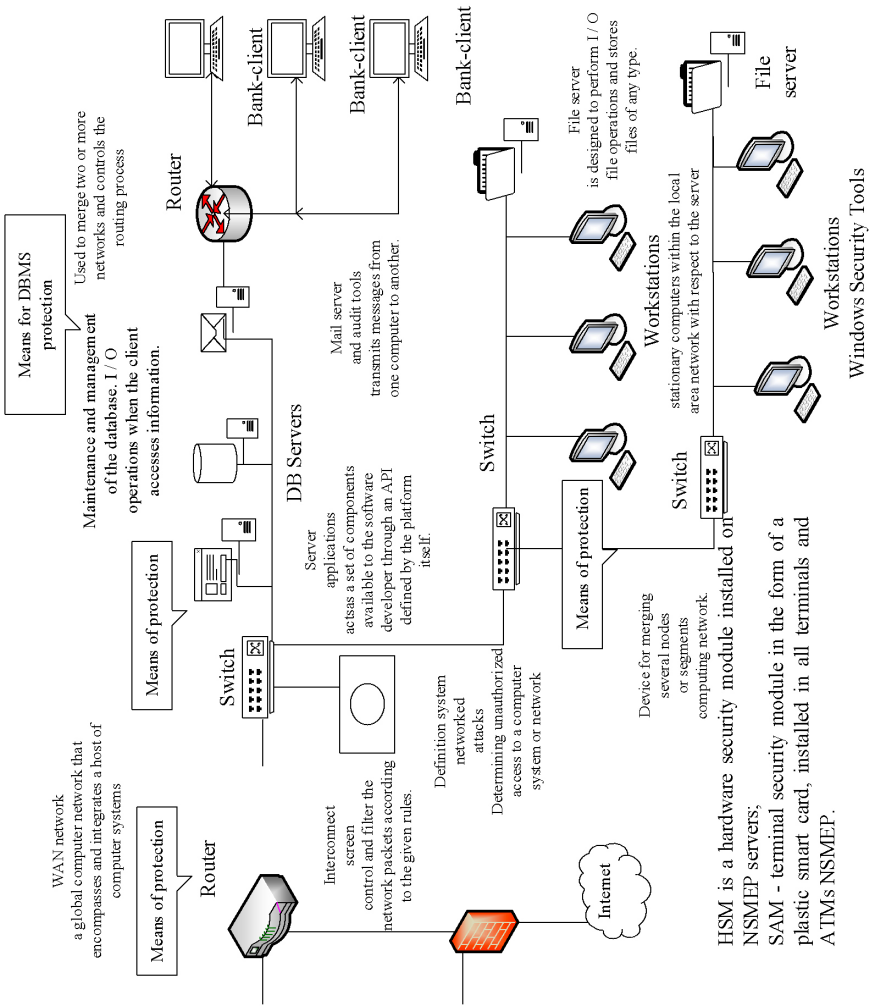


Fig. 1.15. Block diagram ISMS NMEPS

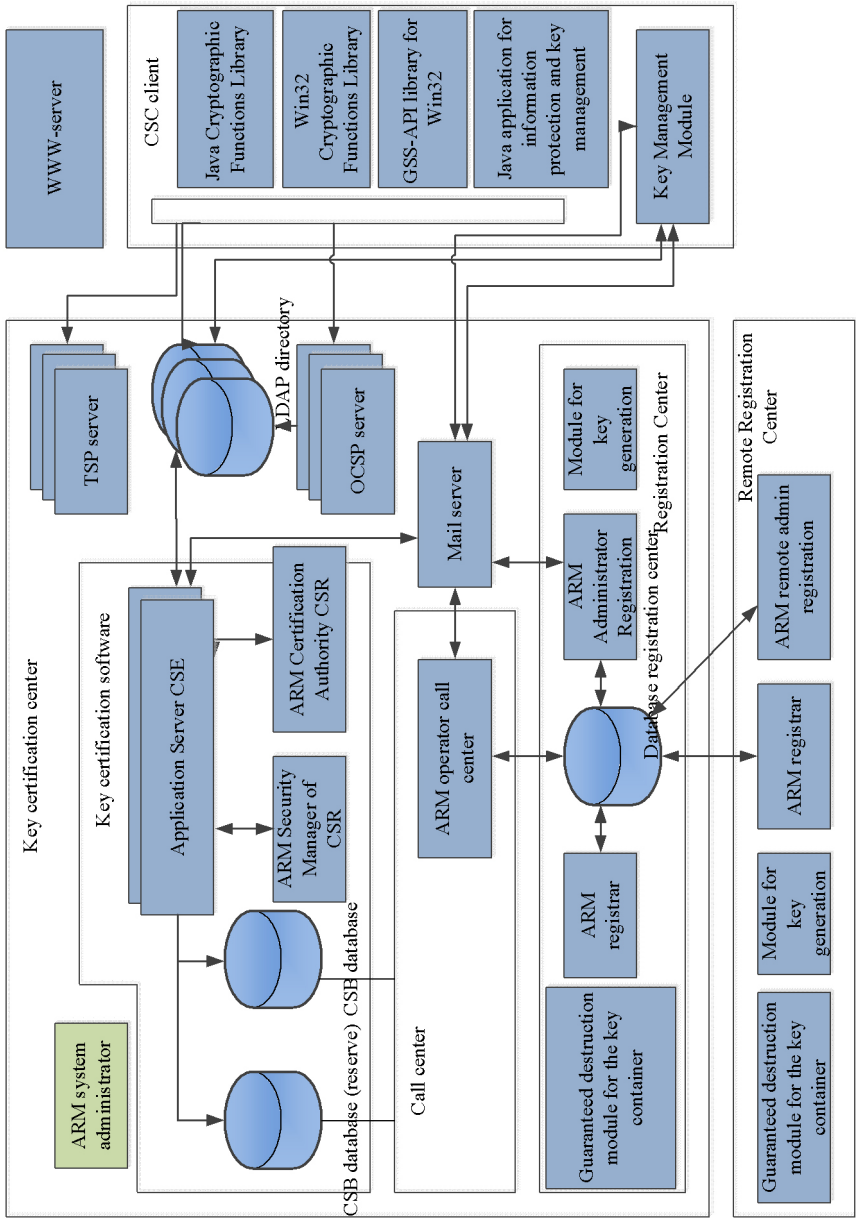


Fig. 1.16. General scheme CIPF "Code-X.509"

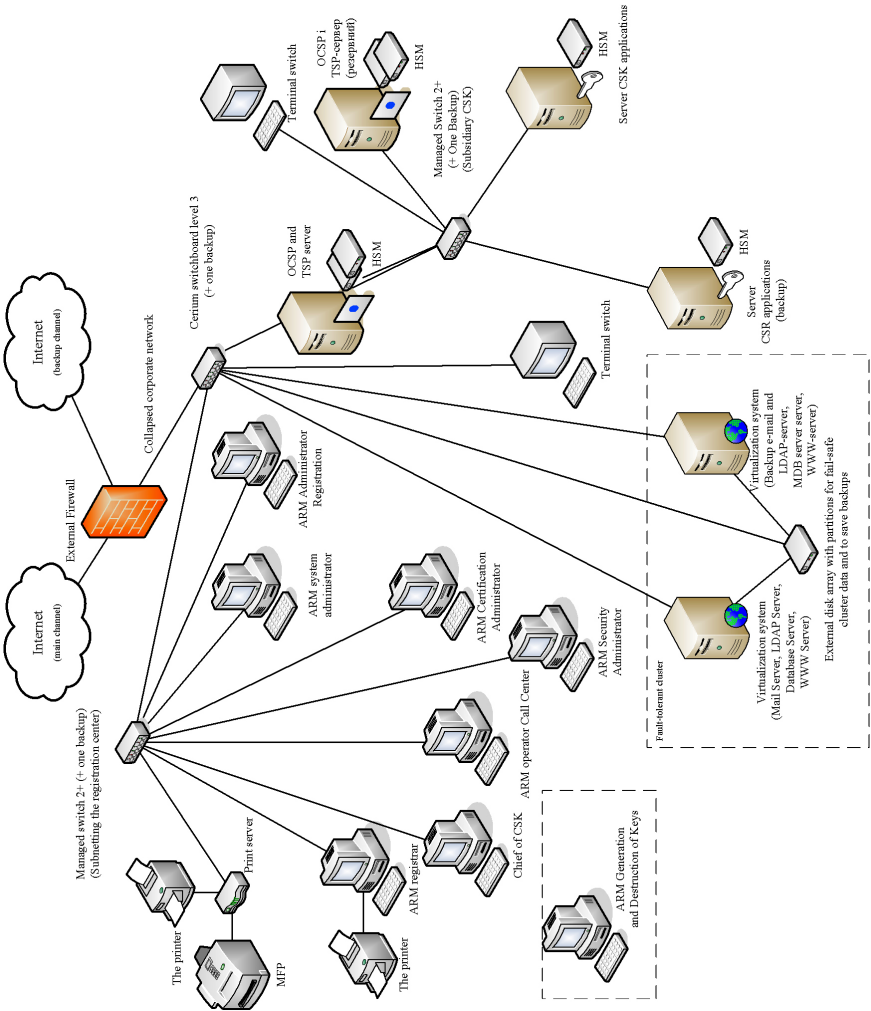


Fig. 1.17. Typical network topology CIPF "Code-X.509"

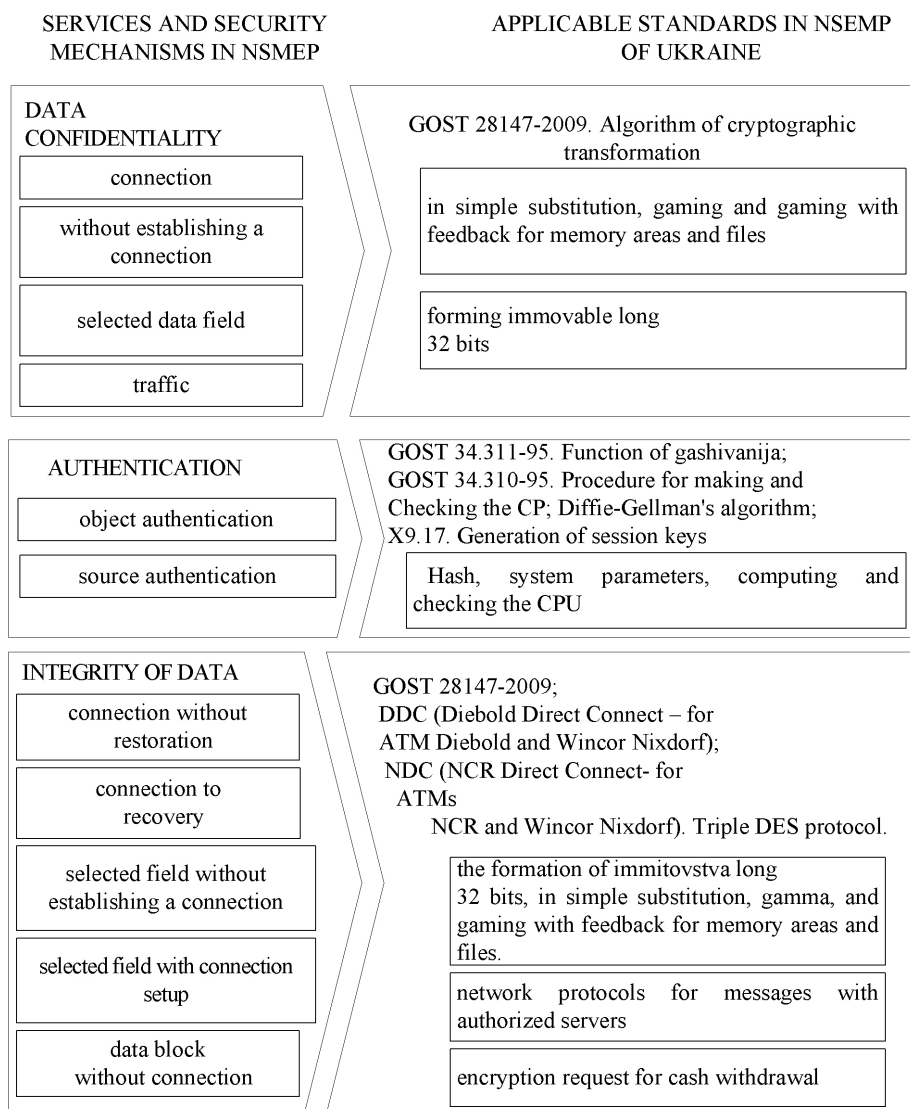


Fig. 1.18. The relationship between the security services and mechanisms NMEPS

Examples of program implementation of the mechanism is a software cryptographic protection “Griffon B” and “Griffon L” intended for cryptographic protection of confidential information in automated banking systems and is used for sharing information within a corporate network bank clients who work with the system “Client-bank” systems servicing plastic cards [31, 69, 70].

The software cryptographic protection of information “Griffon L” [69] intended for use in banking, in particular for the exchange of confidential (including financial) information within a corporate network of the bank, with customers working on the system “Client-Bank” systems servicing plastic cards and others.

Library of cryptographic protection “Typhoon-PKCS # 11” contains procedures designed to protect the integrity and confidentiality of information, perform authentication of senders of messages using mechanisms encryption (digital signature, encryption, making message authentication code and hash functions) by embedding a specific application systems [60].

The procedures are part of the library realize:

- encrypt/decrypt data algorithm GOST 28147–2009;
- production/checking authentication code algorithm GOST 28147–2009;
- generation/verification algorithms for electronic ISO 4145–2002, GOST 34.310–95, 34.311–95;
- develop key encryption scheme Diffie-Hellman (using the open distribution of keys accordance with ISO 11166–94).

Speed characteristics of software tools that implement cryptographic algorithms (for PC based on Intel Celeron 2.4 GHz):

- speed encryption/decryption data in simple replacement BSC GOST 28147–2009 least 8 MB/s;
- speed calculating hash data to GOST 34.311–95 at least 3 MB/s;
- DS formulation according to GOST 34.310–95 with key length of 512 bits with no more than 0.003;
- checking electronic accordance with GOST 34.310–95 key length of 512 bits with no more than 0.006;
- DS formulation according to GOST 34.310–95 at 1024 bit key less than 0.01 seconds;
- checking the electronic signature in accordance with GOST 34.310–95 at 1024 bit key less than 0.02 seconds;
- DS formulation (the calculation presignature) according to ISO 4145–2002 for the main field of 163 degrees with no more than 0.0068;
- When checking the electronic signature according to ISO 4145–2002 for the main field of 163 degrees at most 0.013 sec.

Cryptographic transformation library “Typhoon-PKI PKCS # 11” are implemented using software libraries procedures for cryptographic protection of information “Typhoon-W32” version 2.01.

The system of secure e-mail “Breeze” is designed to exchange electronic messages in a format SMF-70 protected using mechanisms encryption (digital signature, encryption/decryption, making message authentication code)

between email clients (CM) registered on the nodes CM via the arbitrary data types and the criteria ND TPI 2.5–004–99 [71].

To improve information security requirements for information systems of banks, taking into account current cyber threats, setting requirements for organizing the information security and cyber bank, the National Bank of Ukraine [34] defined the basic mechanisms that can be used to provide security services — symmetric cryptography cryptographic algorithms (GOST 28147–2009 “Kalina-256”, AES, with a key length of at least 128 bits — to ensure the confidentiality and integrity of data), asymmetric cryptography (Diffie-Hellman algorithm El-Gamal, both ordinary and elliptic curve algorithm RSA, with a length of 2048 bits primes — providing key exchange) (providing authentication based on MAC codes “Bush” (ISO 7564), SHA-224, SHA-256, SHA-384, SHA-512, methods of strict authentication CPU ISO-4145). Analysis of the proposed changes to the software shows a significant increase in the level of reliability requirements, the use of national standards and algorithms on elliptic curves, providing an extra level of stability (see Fig. 1.5).

Thus, analysis services and mechanisms IS BI in ABS says that their software is typically used BSC and asymmetric cryptography algorithms. Growing threats, their synergy and hybridity on component safety: IS, CB, SI demanding higher level of reliability, which in turn leads to lower quality customer service (business) ABS, reducing public confidence in banking institutions, the emergence items chaos of society, which leads to lower IS state.

1.2 Substantiation of the dissertation

The analysis of the legal framework governing the construction of systems for IS BI in ABS gave reason to identify the main outstanding tasks of IS BI in ABS (applies to both international OBS in general and OBS Ukraine in particular):

- 1) considered only certain components of the methodology of evaluation safety of information technology applied in OBS;

- 2) the absence of a synergistic approach to risk analysis, assessment methodology common information technology security standards in the banking sector does not allow timely develop appropriate policies, new approaches and measures to ensure information security BI;

- 3) lack of consideration IS model (model CIA) an integral part of banking transactions — authentication services;

- 4) no evaluation of protection mechanisms BI in ABS on hybrid integration of an attack based on the signs of threats IS, CS, SI BI to the ABS technical objects of infrastructure;

5) to ensure the integrity and confidentiality of the ABS used “outdated” symmetrical BSC — GOST-28147, 3DES, and asymmetric cryptosystem RSA, Diffie-Hellman, the first problem of distribution mechanisms encryption keys, the second low speed encryption (3–5 orders of magnitude lower than in BSC), but the use of integrated mechanisms allows crypto conversion provide speed, security and reliability BI in ABS.

Thus, based on the needs of compliance with the rules of the threefold position to ensure the safety of BI within a synergistic approach to the interaction of selected security profiles and to enhance its security estimated value risk equivalent monetary capital, meaning the proposed approach in its most general form can be represented as a certain conditional shape (Fig. 1.19).

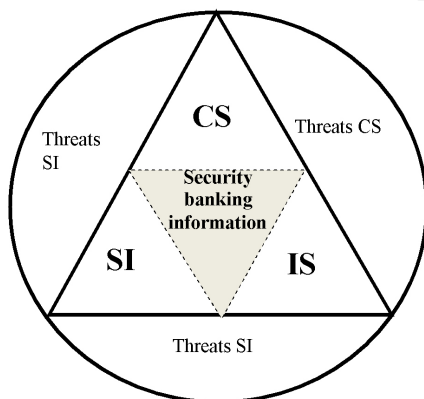


Fig. 1.19. The essence of the synergistic approach to security BI

Note key characteristic feature only offered a synergistic approach to security of banking information, the proposed approach is not simple integration of capabilities safety, it is also not a superposition of their properties. The main objective of the proposed approach — it's excitement in the system of banking information managed emergent properties aimed at obtaining synergies, achieved thanks to a qualitatively new approach to security. Development of this approach is impossible without the development of a common methodology for constructing the security system of banking information, based on deep scientific elaboration of problems through its comprehensive and critical analysis on the basis of the findings, the synthesis of new non-trivial solutions. Today, as shown by the analysis, both in theory and practice of banking information security similar methodology available.

Given the different nature of threats to selected profiles provide banking security and in the interests of obtaining further risk assessments size equivalent monetary capital directly reflects its protection, as proposed introduction of a synergistic index of banking information security in ABS (Fig. 1.20).

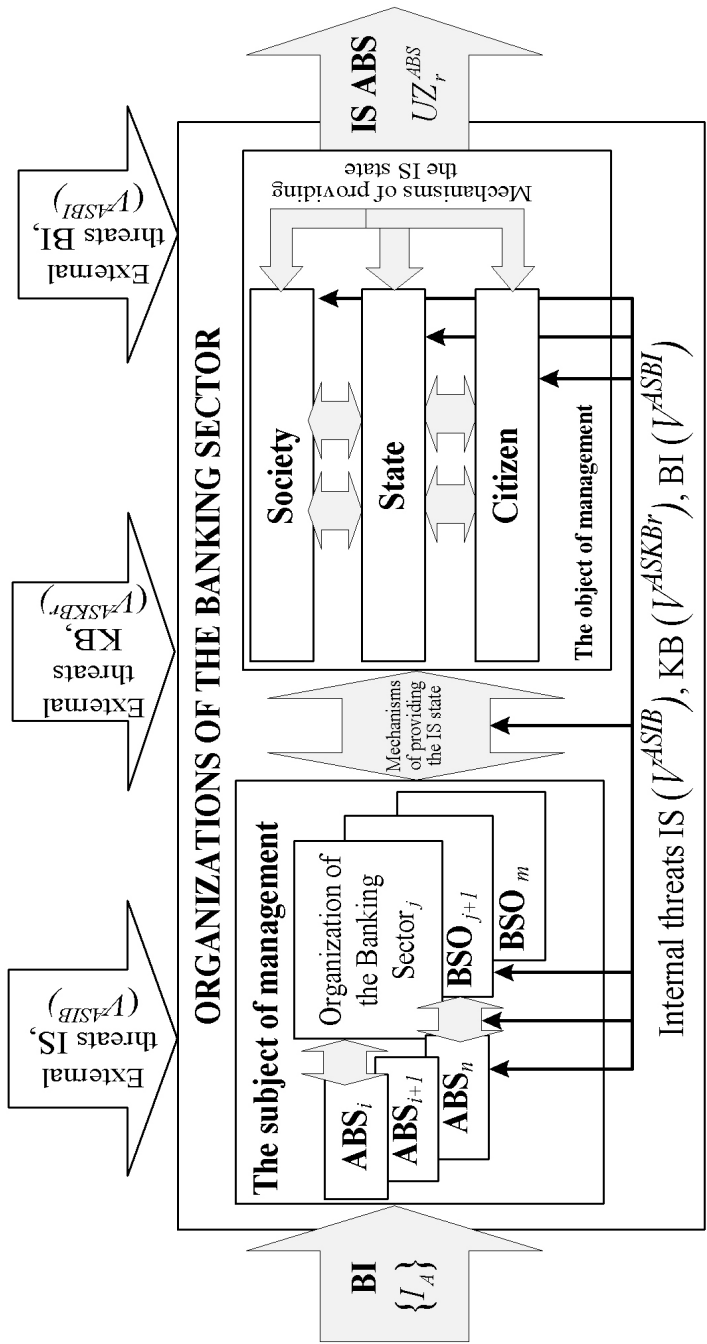


Fig. 1.20. Role of synergistic safety indicators BI in modern banking systems of protection ABS

Synergetic indicator banking information security in ABS — a synergetic assessment of the effectiveness of complex application capabilities banking information security in terms of antagonistic counteraction system of bank protection random and targeted security threats.

It is known that solving the problem of information security of the state as a whole and IS BI ABS devoted to particular works of famous domestic and foreign scientists and their research schools: V. Burachki, S. Buchyka, I. Gorbenko, R. Grischuk, V. Dudykevych, V. Zadiraka, O. Korchenko, A. Kuznetsov, V. Lakhno, S. Lenkova, A. Moldoveanu, V. Mohorje, O. Novikova, A. Petrov, A. Poti, V. Sidelnikov, A. Stasiuk, S. Timofeeva, V. Khoroshko, M. Shelest, A. Yudin, M. Shelest, B. Schneier, B. Shokalo, V. Yarochkyna and many others. Along with being found that the unresolved aspects of the problem for IS state remains the problem of creating a coherent scientifically based methodology for constructing systems for IS BI in ABS implementation in practice which will promote sustainable and stable development of the banking sector of the state.

1.3 Formulation of the problem

Lack currently appropriate methodology also due to the presence contradiction, which determined that on the one hand the practice requires a theory of new approaches to security of banking information in terms of the increasing number of threats to cyber and information security, and information security, while increasing their technological difficulty.

On the other hand, no complete theory scientifically based methodology of practical security system of banking information in general, due to the imperfection of mechanisms to ensure information security, information security and cybersecurity in particular (Fig. 1.21) [47, 49, 53, 54].

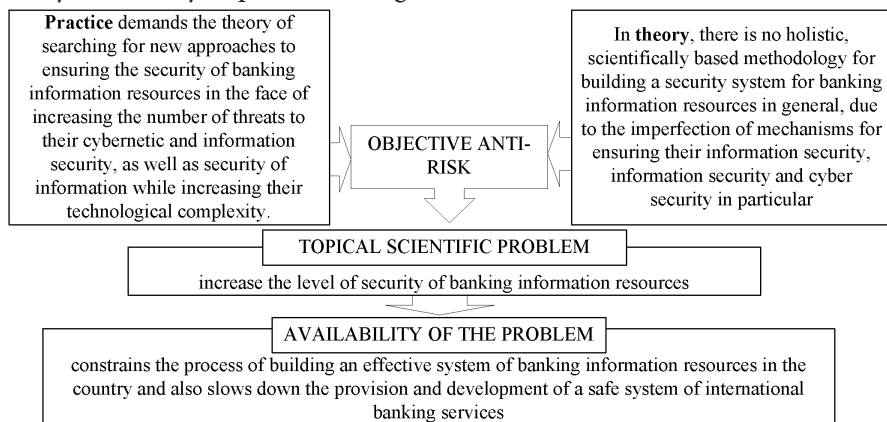


Fig. 1.21. The essence of the scientific problem

Formalized scientific problem can be described by the expression:

$$Emerdg = \max \left\{ \prod_{synerg}^M \right\}, \quad (1.1)$$

where $\left\{ \prod_{synerg}^M \right\}$ — maximum number of emergent properties of the system of banking security in general achieved when a synergistic effect of the interaction of selected security profiles, N — number of states of the security system of banking information or the number of emergent properties, $M \leq N$.

The maximum number of emergent properties of the system of banking security as a whole can be achieved with the condition: $\prod_{synerg}^M = \sum_{m=1}^M C_N^m$.

It is necessary to solve the problem so improving the security of banking information under given conditions to get the maximum number of emergent properties at minimal cost resource aimed at excitation system synergies.

So, today the prevailing objective contradiction between the growing practice requirements for IS BI in ABS, while the increasing number and complexity of technological threats and their entry signs hybridity on the one hand, and imperfect, and sometimes the lack of methodology for constructing systems for IS BI the ABS from such threats on the other. The presence of this contradiction makes the relevance of the dissertation topic, and therefore solve scientific and applied problems is of great scientific and practical importance.

1.4 Conclusions of the first chapter

Thus, in the first chapter of the thesis was an analysis of the scientific literature on the topic of the thesis, including analysis of modern approaches to IT security infrastructures critical state in various fields, particularly in the banking sector. The studies yielded the following results:

1. Analysis of current models, methods and systems for information security in the banking information ABS OBS as part of the critical infrastructure cybernetic state. It is established that the vast majority of known studies focused on the development or general approaches to IS BI in ABS or create methods, models and tools provide model-based CIA, which does not fully take into account modern requirements and approaches to building a system for IS BI in ABS.
2. Unresolved part of the overall problem with BI questions remain coherent development of scientifically grounded methodology for constructing practical systems for IS BI in ABS, development and implementation of a comprehensive information security system (CISS) integrated mechanisms of ISS software requirements for speed and likelihood of circulation in the BI ABS.

3. The results of the analysis made it possible to clearly define the objectives of the research to develop the methodology for constructing systems for IS BI in ABS.

References in Chapter 1

1. *G. V. Grishchuk, Yu. G. Danik* Osnovy kiberneticheskoy bezopasnosti. Monografiya/edited by Yu. G. Dannik. – Zhitomir: ZhNAEU, 2016.
2. *N. L. Volkovskiy* Istoriya informatsionnykh voyn. P. 2. – SPb.: OOO “Izdatel'stvo «Poligon»”, 2003.
3. *E. S. Pelevina* Informatsionnye ugrozy kiberterrorizma//Evraziyskiy Soyuz Uchenykh (ESU), № 11 (20). Politicheskie Nauki, p. 100–103, 2015.
4. *A. A. Bok, D. A. Nikolaeva* Nekotorye voprosy bor'by s kiberprestup-nost'yu v Germanii. URL: <http://cj.isea.ru/pdf.asp?id=8613>. Accessed on: 11.12.2017.
5. *A. V. Korotkov, E. S. Zinov'eva* Bezopasnost' kriticheskikh informat-sionnykh infrastruktur v mezhdunarodnom gumanitarnom prave. URL: <http://cyberleninka.ru/article/n/bezopasnost-kriticheskikh-infor-matsionnyh-infrastruktur-v-mezhdunarodnom-gumanitarnom-prave>. Accessed on: 11.12.2017.
6. *E. V. Ivanchenko, V. A. Khoroshko* Tendentsii razvitiya kiberterrorizma. MNPK “Sovremennye informatsionnye i elektronnye tekhnologii”. – Odes-sa, p. 105–106, 2014.
7. *E. A. Maslakova* Kiberterrorizm kak novaya forma terrorizma//Nauka i Praktika, № 2 (63), p. 79–81, 2015.
8. Kiberataki islamskogo gosudarstva (IGIL) na ob'ekty i kompanii Rossiys-koy Federatsii. URL: http://www.inside-zi.ru/pages/3_2015/22.html. Ac-cessed on: 11.12.2017.
9. *A. Korolev* Kiberprostranstvo i informatsionnyy terrorizm. URL: <http://vpoanalytics.com/2016/02/15/kiberprostranstvo-i-informacionnyj-terrorizm>. Accessed on: 11.12.2017.
10. Nekotorye aspekty kiberterrorizma. URL: <http://nk.org.ua/geopoliti-ka/nekotoryie-aspektyi-kiberterrorizma-16846>. Accessed on: 11.12.2017.
11. Uniting and Strengthening America by Providing Appropriate Tools Re-quired to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. H. R. 3162.
12. *G. P. Leonenko, A. Yu. Yudin* Problemy obespecheniya informatsionnoy bezopasnosti sistem kriticheski vazhnoy informatsionnoy infrastruktury Ukrainy//Information Technology and Security, № 1 (3), p. 44–48, 2013.
13. *A. V. Dorofeev, A. S. Markov* Planirovanie obespecheniya nepreryvnosti biz-nesa i vosstanovleniya//Voprosy kiberbezopasnosti, № 3 (11), p. 68–73, 2015.

14. A. V. Barabanov, A. V. Dorofeev, A. S. Markov, V. L. Tsirlov *Sem' bezopasnykh informatsionnykh tekhnologiy*/edited by A. S. Markova. – M.: DMK Press, 2017.
15. V. S. Olad'ko, S. Yu. Mikova *Strategii i pokazateli obespecheniya nepreryvnosti biznesa*//Mezhdunarodnyy nauchnyy zhurnal, № 7. Tekhnicheskie nauki, p. 109–112, 2016.
16. A. Bashnin *Situativnoe upravlenie i nepreryvnost' biznesa. Situatsionnye tsentry*. P. 3. URL: <http://upr.ru/article/kontseptsii-i-metody-upravleniya>. Accessed on: 11.12.2017.
17. ISO/IEC 27031:2011 Information Technology – Security Techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity. URL: http://www.iso.org/iso/ru/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374. Accessed on: 09.12.2017.
18. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534. Accessed on: 09.12.2017.
19. The doctrine of information security of Ukraine, approved by the Decree of the President of Ukraine dated February 25, 2017, No. 47/2017. URL: <http://zakon3.rada.gov.ua/laws/show/47/2017/paran2#n2>.
20. Decree of the President of Ukraine dated March 15, 2016, No. 96 “On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016, On the Strategy of Cybersecurity of Ukraine”. URL: <http://zakon3.rada.gov.ua/laws/show/96/2016/paran11#n11>.
21. Decree of the President of Ukraine dated February 12, 2007 No. 105 “On the Strategy of National Security of Ukraine”. URL: <http://zakon3.rada.gov.ua/laws/show/105/2007>.
22. R. V. Grishchuk, Yu. G. Danik *Sinergiya informatsionnykh i kiberneticheskikh deystviy*//Proceedings of the NUOU, № 6 (127), p. 132–143, 2014.
23. V. L. Buryachok, R. V. Grishchuk, and V. A. Khoroshko *Politika informatsionnoy bezopasnosti*/edited by prof. V. A. Khoroshko. – K.: ChPP «Zadruga», 2014.
24. Yu. G. Danik et al. *Osnovy zashchity informatsii*. Tutorial. – Zhitomir: ZhVI DUT, 2015.
25. A. K. Yudin *Informatsionnaya bezopasnost'. Normativno-pravovoe obespechenie*. – M.: NAU, 2011.
26. I. S. Ivanchenko, V. A. Khoroshko, Yu. E. Khokhlachova, D. V. Chirkov *Obespechenie informatsionnoy bezopasnosti gosudarstva*/edited by prof. V. A. Khoroshko. – K.: ChPP “Zadruga”, 2013.

27. A. G. Korchenko, A. E. Arkhipov, Yu. A. Dreys Otsenivanie vreda natsional'noy bezopasnosti Ukrainy v sluchae utechki gosudarstvennoy tayny. Monografiya. – K.: NA SBU Ukrainy, 2014.
28. A. A. Korchenko, L. N. Skachek, V. A. Khoroshko Bankovskaya bezopasnost. Uchebnik/edited by prof. V. A. Khoroshko. – K.: ChPP “Zadruga”, 2014.
29. V. I. Yarochkin Bezopasnost' bankovskikh sistem. – M.: Publisher: Os'-89, 416 p., 2012.
30. S. Evseev Analiz zashchity v natsional'noy sisteme masovykh elektronnykh platezhey//Informatsionnaya bezopasnost', № 3 (15), № 4 (16), p. 15–28, 2014.
31. S. Evseev, O. Korol', G. Kots Analiz zakonodatel'noy bazy k sisteme upravleniya informatsionnoy bezopasnost'yu NSMEP//Vostochno-evropeyskiy zhurnal передovykh tekhnologiy, ed. 5/3 (77), p. 48–59, 2015.
32. S. Evseev Metodologiya otsenivaniya bezopasnosti informatsionnykh tekhnologiy avtomatizirovannykh bankovskikh sistem Ukrainy// Nauchno-tekhnicheskiiy zhurnal “Zashchita informatsii”, vol. 22, № 2, p. 297–309, 2016.
33. R. Grishchuk, S. Evseev The synergetic approach for providing bank information security: the problem formulation//Informatsionnaya bezopasnost', № 22 (1), p. 64–74, 2016.
34. Postanovlenie NBU 28.09.2017 № 95, “Ob utverzhdenii Polozheniya ob organizatsii meropriyatiy po obespecheniyu informatsionnoy bezopasnosti v bankovskoy sisteme Ukrainy”. URL: <http://zakon2.rada.gov.ua/laws/show/en/v0095500-17/page>. Accessed on: 5.12.2017.
35. S. Evseev, Yu. Khokhlacheva, and O. Korol' Otsenka obespecheniya nepreryvnosti biznes-protsessov v organizatsiyakh bankovskogo sektora na osnove sinergeticheskogo podkhoda, P. 1//Sovremennaya spetsial'naya tekhnika. Nauchno-prakticheskiiy zhurnal, № 1 (48), p. 17–25, 2017.
36. S. Evseev, Yu. Khokhlacheva, and O. Korol' Otsenka obespecheniya nepreryvnosti biznes-protsessov v organizatsiyakh bankovskogo sektora na osnove sinergeticheskogo podkhoda, P. 2//Sovremennaya spetsial'naya tekhnika. Nauchno-prakticheskiiy zhurnal, № 2 (49), p. 10–17, 2017.
37. S. S. Khimka Razrabotka modeley i metodov dlya sozdaniya sistemy informatsionnoy bezopasnosti korporativnoy seti predpriyatiya s uchetom razlichnykh kriteriev. URL: <http://masters.donntu.org/2009/fvti/khimka/diss/index.htm>. Accessed on: 7.12.2017.
38. Ukrainian security resource. URL: <http://kiev-security.org.ua>. Accessed on: 7.12.2017.
39. D. Slobodenyuk “Banking technologies, Information security tools in banking systems”, [Online] Available: <http://www.arinteg.ru/about/>

- publications/press/sredstva-zashchity-informatsii-v-bankovskikh-sistemakh-131107.html. Accessed on: Dec. 7.2017.
40. *M. N. Simakov* V S"ezd direktorov po informatsionnoy bezopasnosti, [On-line]. Available: http://www.cso-summit.ru/data/2012/presentations/cso2012_013_express-tula_simakov.pdf. Accessed on: Dec. 7.2017.
 41. *P. V. Revenkov* Zashchita informatsii v banke: osnovnye ugrozy i bor'ba s nimi. URL: <http://www.crmdaily.ru/novosti-rynka-crm/568-zashchita-informacii-v-banke-osnovnye-ugrozy-i-borba-s-nimi.html>. Accessed on: 7.12.2017.
 42. Security of Internet Banking – A Comparative Study of Security Risks and Legal Protection in Internet Banking in Thailand and Germany. URL: <http://www.thailawforum.com/articles/internet-banking-thailand.html>. Accessed on: 09.12.2017.
 43. *M. V. Starinskiy* Ob opredelenii ponyatiya "bankovskaya informatsiya" i vydelenie ee vidov. URL: uabs.edu.ua/images/.../K.../Starinskii_s_015.pdf. Accessed on: 7.12.2017.
 44. *S. P. Evseev, O. G. Korol', G. P. Kots* Analiz zakonodatel'noy bazy k sisteme upravleniya informatsionnoy bezopasnost'yu NSMEP//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, Ed. 5/3 (77), p. 48–59, 2015.
 45. *V. A. Serdyuk* Novoe v zashchite ot vzloma korporativnykh sistem. – Moscow: Tekhnosfera, 2007.
 46. *S. Evseev, B. Tomashevskyy* Two-factor authentication methods threats analysis//Radioelektronika, informatika, upravlenie, Ed. 1 (32), p. 52–60, 2015.
 47. *R. V. Grishchuk* Sintez sistem informatsionnoy bezopasnosti s zadannymi svoystvami//Vestnik Natsional'nogo universiteta "Lvovskaya politehnika". Series: Avtomatika, izmereniya i upravleniya: LP, № 74, p. 271–276, 2012.
 48. *R. V. Grishchuk* Ataki na informatsiyu v informatsionno-kommunikatsionnykh sistemakh//Sovremennaya spetsial'naya tekhnika, № 1 (24), p. 61–66, 2011.
 49. *R. V. Grishchuk, and V. V. Okhrimchuk* Postanovka nauchnoy zadachi po razrabotke shablonov potentsial'no opasnykh kiberatak//Bezopasnost' informatsii, Vol. 21, № 3, p. 276–282, 2015.
 50. *Yu. G. Danik, R. V. Grishchuk* Sinergeticheskie efekty v ploskosti informatsionnogo i kiberneticheskogo protivoborstva. Nauchno-prakticheskoy. konf. "Aktual'nye problemy upravleniya informatsionnoy bezopasnost'yu gosudarstva". – Kiev, 19 march 2015, p. 235–237.
 51. *R. V. Grishchuk, V. V. Okhrimchuk* Napravleniya povysheniya zashchishchennosti komp'yuternykh sistem i setey ot kiberatak. II Mezhdunar. nauchno-prakticheskoy. konf. "Aktual'nye voprosy obespecheniya kiber-

- bezopasnosti i zashchity informatsii” (Zakarpatskaya oblast, Mukachevskiy rayon, selo Verkhnee Studenoe, 24–27 febr. 2016). – M.: Izdatel'stvo Evropeyskogo universiteta, p. 60–61, 2016.
52. *Rodzher, Everett M.* Diffuziya innovatsiy. Ed. “Kievo-Mogilyanskaya akademiya”, 2009.
53. *A. A. Kolesnikov* Sinergeticheskoe metody upravleniya slozhnyimi sistemami: teoriya sistemnogo sinteza. – M.: Editorial URSS, 2005.
54. *G. Khaken* Sinergetika. Ierarkhiya neustoychivostey v samoorganizuyushchikhsya sistemakh i ustroystvakh. – M.: Mir, 1985.
55. *A. V. Serikov* Effektivnost' khozyaystvennoy deyatel'nosti: opredelenie, izmerenie, sinergeticheskoy upravlenie//*Ekonomicheskij vestnik Donbasa*, № 2 (24), p. 212–219, 2011.
56. *V. G. Olifer, N. A. Olifer* Bezopasnost' komp'yuternykh setey. – M.: Goryachaya liniya. Telekom, 2015.
57. Otchet CERT-UA za 2010–2013 gody. URL: <http://cert.gov.ua/?p=316>. Accessed on: 7.12.2017.
58. Kibershchit Ukrainy: kto stoit na strazhe kibergranits strany. URL: <http://zillya.ua/ru/kibershchit-ukrainy-kto-stoit-na-strazhe-kibergranits-strany>. Accessed on: 7.12.2017.
59. *W. Ten, G. Manimaran, and C.-C. Liu* Cybersecurity for critical infrastructures: Attack and defense modeling//*IEEETrans. Syst., Man Cybern. A*, vol. 40, no. 4, p. 853–865, 2010.
60. *S. V. Lenkov, D. A. Peregudov, V. A. Khoroshko* Metody i sredstva zashchity informatsii. Monografiya [in 2 vol.], Vol. 2. Informatsionnaya bezopasnost'. – K.: Ariy, 2008.
61. Metodicheskie rekomendatsii po vnedreniyu sistemy upravleniya informatsionnoy bezopasnost'yu i metodiki otsenki riskov v sootvetstvii so standartami Natsional'nogo banka Ukrainy. URL: zakon.rada.gov.ua/laws/show/v0365500-11. Accessed on: Dec. 7.12.2017.
62. Worldwide Infrastructure Security Report. 2014. Arbor Networks, Inc. URL: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=http%3A%2F%2Fpages.arbornetworks.com%2Frs%2Farbor%2Fimages%2FWISR2014_EN2014.pdf&ei=DyR2VfznJOPgyQOghoN4&usg=AFQjCNGP0_ZTliItqCtofJ-cXfZT9QHRiQ&sig2=4hgA_vIye1idQyQgsTIZXg&bvm=bv.95039771,d.bGQ. Accessed on: 09.12.2017.
63. Bezopasnost' IP-setey novogo pokoleniya dlya provayderov uslug. URL: http://www.eureca.ru/edu/study/cisco/library/download.php?type=pdf&att=IP_NGN.pd. Accessed on: 7.12.2017.

64. *S. P. Evseev* Analiz zashchity v natsional'noy sisteme masovykh elektronnykh platezhey//Informatsionnaya bezopasnost', № 3 (15), № 4 (16), p. 15–28, 2014.
65. *S. Yevseiev, H. Kots, and Y. Liekariev* Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, 6/4 (84), p. 11–23, 2016 (Scopus).
66. *S. Yevseiev, H. Kots, S. Minukhin, O. Korol', and A. Kholodkova* The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, 5/9 (89), p. 19–35, 2017 (Scopus).
67. *S. P. Evseev, and T. A. Sverdlo* Issledovanie ugroz metodov dvukhfaktornoy autentifikatsii. Informatsionnye tekhnologii i zashchita informatsii v informatsionno-kommunikatsionnykh sistemakh: Monografiya/edited by V.S. Ponomarenko. – Kharkov, Ukraine: Ed. Ltd. “Shchedra sadiba plyus”, p. 141–154, 2015 .
68. DSTU ISO/IEC 9594–8: 2006 Informatsionnye tekhnologii. Vzaimosvyaz' otkrytykh sistem. Katalog. Part 8. Osnovnye polozheniya po sertifikatsii otkrytykh klyuchey i atributov. URL: http://document.ua/informaciini-tehnologiyi_-vzaemozvE28099jazok-vidkritih-sist-std10750.html. Accessed on: 7.12.2017.
69. Programmnoe sredstvo kriptograficheskoy zashchity informatsii “Grifon-B”. URL: <http://www.banksoft.com.ua/index.php?id=28>. Accessed on: 7.12.2017.
70. Programmnoe sredstvo “Biblioteka funktsiy kriptograficheskoy zashchity informatsii “Grifon-L””. URL: <http://www.banksoft.com.ua/index.php?id=27>. Accessed on: 7.12. 2017.
71. *S. P. Evseev, V. E. Chevardin, S. A. Radkovskiy* Mekhanizmy obespecheniya autentichnosti bankovskikh dannyykh vo vnutriplatezhnykh sistemakh komercheskogo banka. Sbornik nauchnykh statey KhNEU. – Khar'kov: KhNEU, Ed. 6, p. 40–44, 2008.

CHAPTER 2. Development conceptual foundations of information security of banking information in the automated banking system

2.1 Developing the concept of building a synergetic model of banking information security threats in automated banking systems

In modern conditions the mass availability of computer systems and telecommunications, increased electronic document turnover between banks and customers transition to e-commerce security concerns BI due to natural and artificial factors only aggravated. As a result, losses from security breaches BI becomes more expensive for banks and their customers [1, 2, 46]. For example, the largest number of IT security threats ABS Ukraine, as in other states, comes from the Internet when transferring BI open channels of communication [3, 2, 32, 42, 44, 45]. Gaps in the strategic management of IT security Ukraine poured ABS for public banking sector in a number of problems, the main ones being a lack of system security, lack of coordination mechanisms to ensure IT security ABS, especially in two international and multilateral formats, etc. [4, 41, 42].

Analysis of key international standards and standards of Ukraine [7, 8, 9, 10, 11, 12, 13, 24, 26, 28, 29, 31, 32, 33, 34, 35, 36, 37] showed that examined individual components of the methodology of evaluation of information security technologies used in the banking sector, based on the model of security — integrity, confidentiality and availability (model DCI), while not considered an integral part of banking transactions — authentication service — state bank information in which information provides authentication source (authorized user and/or process) of information. The lack of a synergistic approach to risk analysis, common methodologies safety evaluation of information technology in the standards of the banking sector does not allow timely establish appropriate policies, new approaches and measures to ensure the security BI in ABS, due to imperfect mechanisms for its IS, CB, SI particular, integral part of the problem is a security problem BI risk analysis. In fact, the risk is an integral assessment of how well existing remedies able to withstand attacks on banking information [1, 2, 6, 32, 33, 44, 45, 46, 47, 48, 50]. Despite the fact that the currently developed set of mechanisms and information security, today time one of the priorities is the task of evaluating the effectiveness of the IT security of ABS based on relevant metrics. For example, as shown by analysis [6, 7, 8, 9, 10, 11, 12, 13, 24], among the most common metrics is their safety following taxonomy: Vaughn-Hennig-Siraj, NIST STS822, OCIPEP, OCTAVE, CISWG, Erkan Kahraman.

As a result of these metrics safety study found that their effective implementation in the banking sector restrains Ukraine: definitional uncertainty — due to the imperfection of national legislation and its disagreement with the best international practices in this field; low objectivity of ratings received — because of the lack of international experience mainly bank staff that ensures the safety BI in ABS; methodological problems — because of problematic get harmonized with each other quantitative and qualitative assessments and others [5, 50]. In this last of the problems is system-key character, and therefore requires deep scientific and technical processing and further investigation.

The analysis showed that the main documents that have made significant theoretical and practical contributions to solving problems of information security [6] are: Evaluation Criteria security of computer systems [7], known as the “Pink Book”; European IT security evaluation criteria [8]; Canadian security evaluation criteria reliable computer systems [9]; US Federal criteria [10]; International Standard ISO/IEC 15408 — “Criteria for evaluation of IT security” [11, 12, 13]; The working draft standard CEM-97/017 — “General methodology for evaluating IT security” [34] ISO ISO/IEC TR 13335. Information technology. Guidance on safety management of information technology. Part 1–5 [14, 15, 16, 17, 18], Ukraine Standard GOST ISMS 2.0/ISO/IEC 27002: 2010 Information technology. Methods of protection. Code of Practice for Information Security Management (ISO/IEC 27002: 2005, MOD) [23].

Analysis of the documents confirming the fact that to meet the challenges for IB, along with formal methods of modeling processes and evaluation of the efficiency of security systems, is necessary to use methods of decomposition and structuring components of systems and processes, informal assessment methods and efficiency of decision-making. This means that the device must use systems analysis at all stages of the life cycle of information security systems [46, 50]. A special place in the development of methodology for evaluating the security of information technology in the ABS covers standard ISO/IEC 15408 “General criteria for evaluation of IT security”, “Common Criteria”. The standard specifies the general criteria used as a basis for evaluation of security properties of information products and technologies [11, 12, 13]. The only criteria designed to ensure comparability of results of evaluations obtained by different experts, by introducing a set of general requirements for the security features of products and IT systems, as well as performance of these functions. Using standard that analyzes can solve a specific application problem selecting appropriate performance requirements and IT security [6, 46]. In addition, potential security threats with a single criterion, namely integrity, availability, confidentiality subsequently offered to put a synergistic components of a new model of security

threats. Standards of the National Bank of Ukraine [22, 23] based on international standards ISO 27001 [19] and ISO 27002 [20] adding them to the requirements of data protection [23] due to the specific needs of the banking and legal requirements of national legislation [26]. The key point discussed documents is that they attribute to the principles of information security management of the bank, the most important of which are risk assessment [14, 15, 16, 17, 18, 22, 23, 26]. Practice shows that today we can clearly distinguish two main groups of methods for assessing security risks [19, 20, 23, 28, 29]. The first group of methods allows you to set the level of risk by evaluating the extent to defined set of requirements for information security. As sources of such requirements in the banking sector, Ukraine can serve both international and national guidelines, ordering them by the scheme shown in Fig. 2.1.

The second group of methods for risk assessment IS BI in ABS based on determining the probability of attacks and levels of damage. In this case, the risk value is calculated for each threat and, in general, is a product of the probability of the threat of the magnitude of potential losses from this threat. The value of the loss is measured own BI, and the probability of threats is calculated by the panel conducting the audit procedure.

A distinctive feature of the methods of the first and second groups is the use of different scales for the determination of risk. In the first case, the risk and all its parameters expressed in numerical, i. e. quantitative values. In the second case, use qualitative scale.

According to the standards of the National Bank of Ukraine according to the proposed concept of strategic IT security management ABS Ukraine (Fig. 2.1) the scope of the IS management system (ISMS), which should be implemented, in general, a bank.

The decision of all complex issues related to security in ABS BI Ukraine — namely, IS, CB, SI in the ABS should be solved together and inseparably from each other harmoniously complementing and filling, if necessary, each other. Easy integration of capabilities in each case to ensure the security BI in ABS is impractical both practical and scientific viewpoints. Lack other alternative approaches makes the urgency of solving the problem that has arisen — a more secure BI ABS through the development of new approaches.

Given the relationship hybridity threats IS, CB, SI BI on the ABS, subsequently invited to synthesize typical threats BI by BI threats synergetic model [1] (Fig. 2.2). A distinctive feature of the proposed approach (see Fig. 2.2) is laying the necessary and sufficient conditions for the development of new methodological basis in achieving synergies in the area of safety components, IS, CB, SI BI in ABS in terms of hybrid threats not only to Ukraine, but other developed countries.

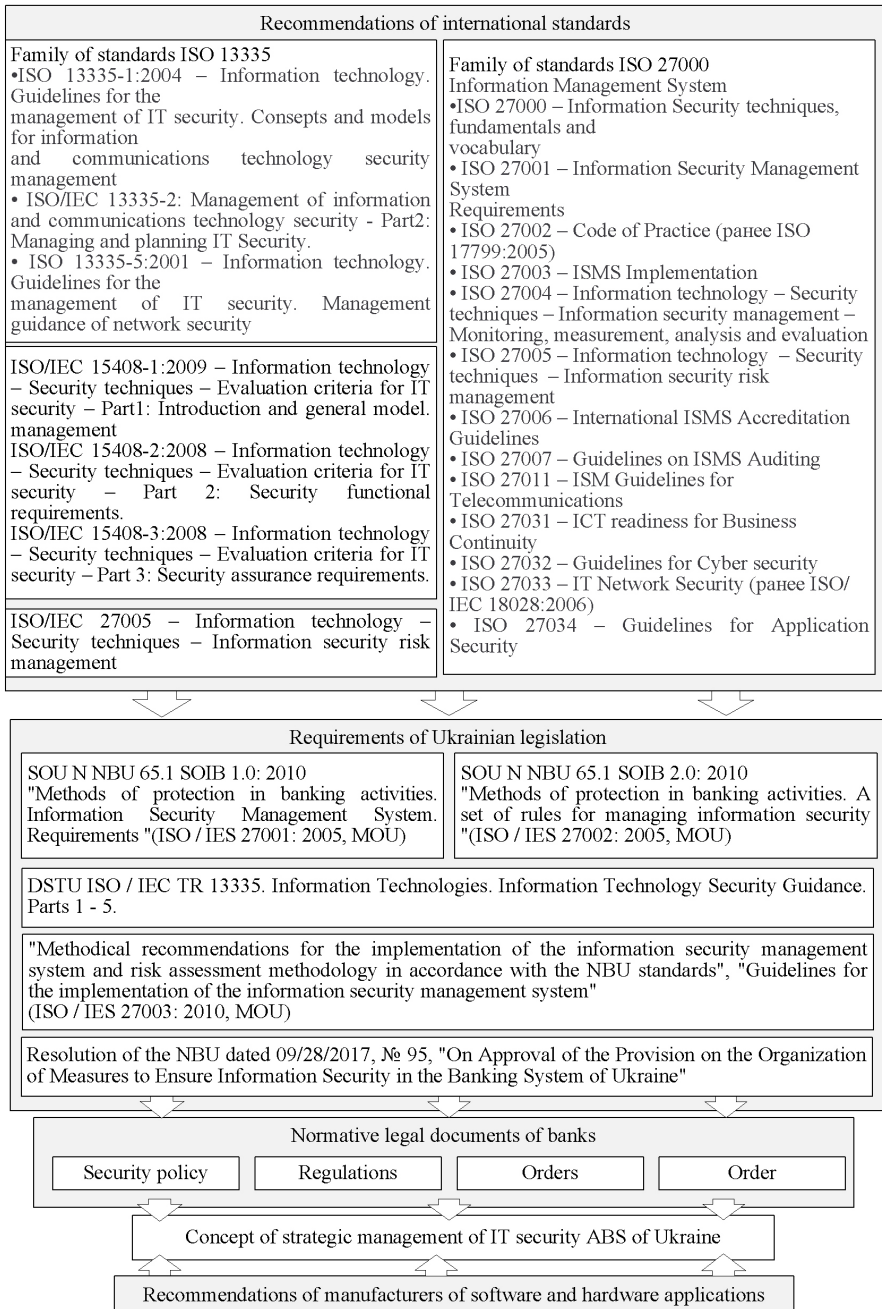


Fig. 2.1. Systematics sources of safety requirements for ABS IT Ukraine

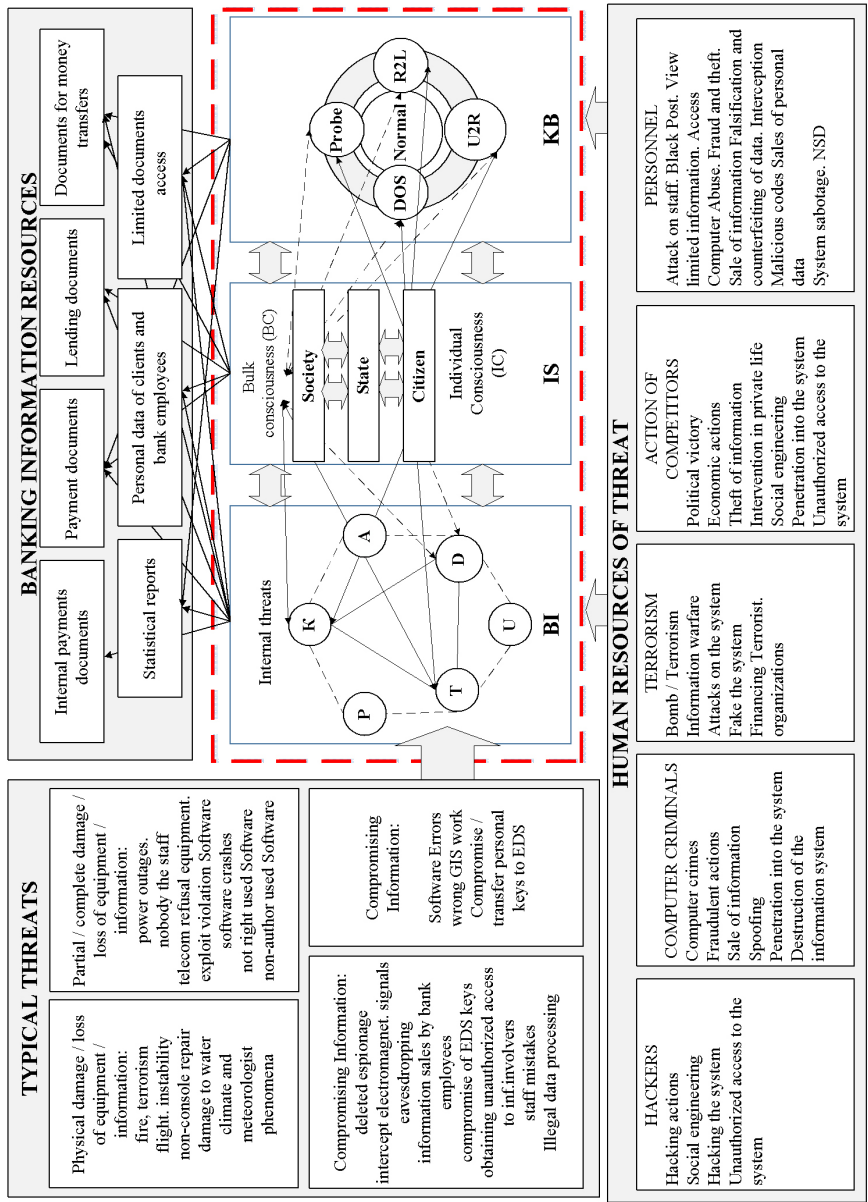
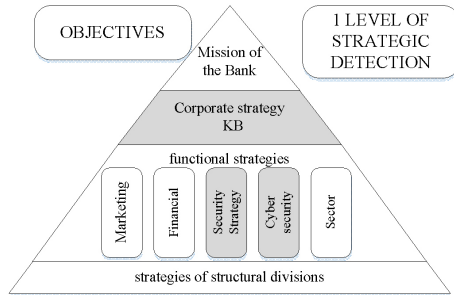


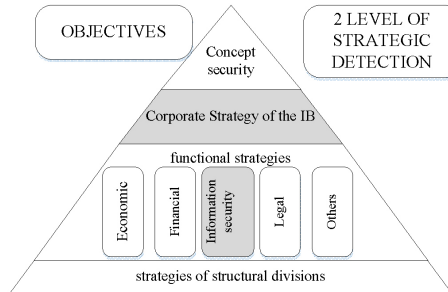
Fig. 2.2. Relationship BI typical sources of threats

Thus, through the amendment of the requirements of advanced international practices in matters of security evaluation methodology BI in ABS established relationship between the main security risks and BI, today and in the near future will take place in Ukraine ABS.

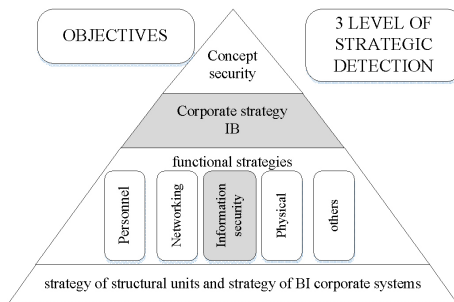
Based on the three-level functional model of strategic set of typical enterprise [4] in order to develop conceptual basis for IS BI in ABS synergetic proposed the concept of building a model of threats IS BI in ABS based on a three-level security management strategy BI in ABS (Fig. 2.3 a, b, c).



a



b



c

Fig. 2.3. The concept of information security threats synergetic model BI in ABS

First level describes the overall corporate strategy of the bank and its functional strategy (see. Fig. 2.3 a). Corporate strategy defines development prospects and serves the core mission of the bank. At this level, according to a synergetic approach the general concept of security of information technology ABS and emerging goals and objectives to ensure KB. This level is determined by the state of IS BI in ABS:

$$S^{ABS} = \{S_1^{ABS}, S_2^{ABS}, \dots, S_m^{ABS}\},$$

where $S_i^{ABS} \in \{S^{ABS}\}, (i = \overline{1, m})$ — state IS BI in ABS. Functional strategies are one of horizontal communication and coordinated at the level of goals, with further detail at the next level strategic set.

The second level is formed corporate strategy IS BI in ABS (Fig. 2.3 b):

$$\{RR^{ABS}\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}, \quad (2.1)$$

where $\{RR^{ABS}\}$ — set of regulatory requirements includes requirements for security BI — $\{R_{BBI}\}$ defined in international and national standards set estimates the extent to which safety requirements $\{OV_{BBI}\}$ and set the final level of safety of BI $\{IU_{BBI}\}$.

Also defined goals and objectives of key business processes relating to the protection of personal data of legal and private clients. Corporate Security Strategy describes how you want to manage and coordinate the efforts of various aspects of security. It develops functional strategies, economic financial, physical and information security.

The third level is made functional strategies detailed second-level strategic set formed corporate information security strategy (see Fig. 2.3).

The main areas to protect advisable to provide personnel security, physical security, network and BI. This level is determined by the correspondence between the applied technical means of information protection (TMIP) and threats IS, CB, SI in a BI ABS:

$$OPZ^{ABS} = \sum_{i=1}^k OPZ_i, \quad (2.2)$$

where OPZ_i — general indicator of the level of security of ABS, to evaluate the level of compliance with the requirements TMIP regulators.

IS strategy is an important function of the bank's management and security should be formed and held senior management.

This concept is based on a synergetic approach to the selection of the most effective ways achieving goals IS BI in ABS to the value of risk at every level model of strategic management of the bank. The approach allows to conduct

comprehensive selection of possible alternatives strategic decisions on security and develop a method of evaluating a generalized indicator of IS BI in ABS, which includes three stages:

1) Defining the impact probability of threats IS, CB, SI information security BI.

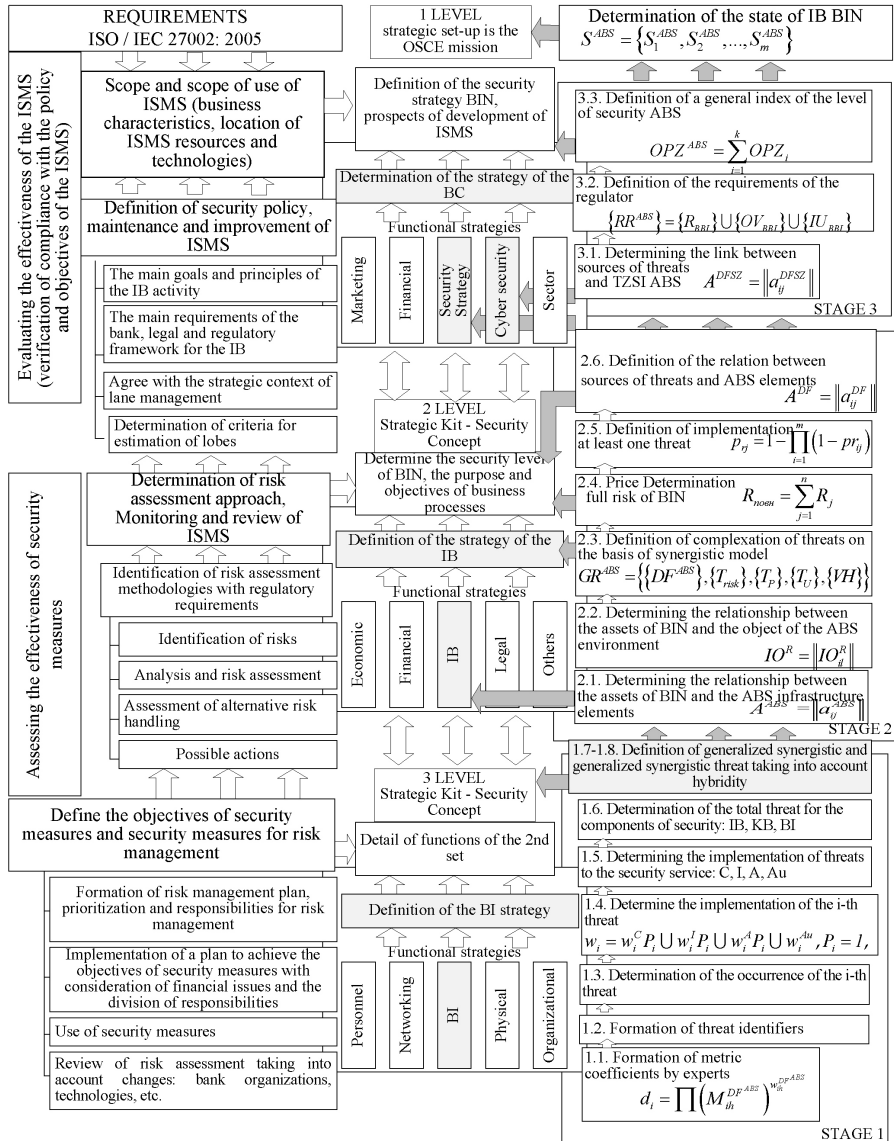


Fig. 2.4. Scheme evaluation methods generalized index of IS BI in ABS

2) Definition of dependencies between elements of infrastructure ABS information assets BI, threats IS, CB, SI and TMIP improved model based infrastructure ABS synergetic model threats, improved model of the attacker.

3) The definition of a generalized indicator of IS BI in ABS model based on improved evaluation of the security BI in ABS, for example of the Ukraine OPS shown in Fig. 2.4.

Developed based on the concept model through integration of the components of information security, cyber security and information security opens a new direction in providing banking information security in automated banking systems based on the model of the strategic management of the bank to the value of risk at every level.

2.2 The formalization of the principles of construction components threats branch banking information security, information security, cyber security, information security

***Step 1.** Determining the impact probability of threats IS, CB, SI information security BI realized on the basis of the proposed classifier.*

To build metrics based threats synergistic approach proposed in [50] use the approach of constructing the classifier threats based information-analytical model of the double triples proposed by the authors in [51, 52, 53, 54]. Unlike well known in the construction of the classifier substantial portion of each of the four platforms include, respectively:

first platform — classification of threats against the security component BI in OPS ABS: information security (IS) (01), security of information (SI) (02), cybersecurity (CS) (03).

We introduce the following definitions:

***Definition 1.** Security banking information (S BI)* — the state of protection of banking information, characterized by the ability of users, hardware and information technology to ensure the confidentiality, integrity, authenticity and availability BI when it is processed in ABS.

***Definition 2.** Information Security banking information (IS BI)* — the state security information OPS environment that ensures its formation, use and development in the interests of citizens and OPS.

***Definition 3.** Cyber banking information (CB BI)* — a set of tools, policies, principles of safety, security guarantees, risk management approaches, actions, training, insurance and technology used to protect cyberspace ABS, resources and users of OPS.

second platform — classification of threats in nature areas: regulatory (01), organizational (02), engineering (03);

third platform — classification of threats in accordance with the basic features of information: privacy (01), integrity (02), availability (03), authenticity (04);

fourth platform — classification by level hierarchy of threats infrastructure ABS: PHL — the physical layer (01), NL — network layer (02), OSL — level operating systems (OS) (03), DBL — level database management systems (04), BL — level banking technology applications and services (05).

Part of the classifier divided point and have the form shown in Fig. 2.5.

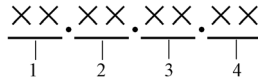


Fig. 2.5. The components of the generalized classifier:

- 1 — synergistic component security BI; 2 — nature areas;
3 — Features information; 4 — level hierarchy infrastructure ABS

Fig. 2.6 given the relationship block diagram of the classifier threats ABS OPS. The set of threats IS, CB, SI BI at the ABS prompted use of electronic resources (<http://bdu.fstec.ru/vul>).

Step 1.1 Formation metric coefficients expert threats for security services:

$$d_i = \Pi \left(M_{ih}^{DF^{ABS}} \right)^{w_{ih}^{DF^{ABS}}}, \quad (2.3)$$

where $M_{ih}^{DF^{ABS}}$ — the value of h -oh metric of i -offender;

$w_{ih}^{DF^{ABS}}$ — weighting metrics h -oh i -th offender $\sum_h w_{ih}^{DF^{ABS}} = 1$.

Step 1.2 Formation identifiers threats on classifier components.

At this step, experts form the numerical value (code) of the threat ID for the relevant components of the classifier.

Step 1.3 Determining the occurrence probability PI i -th threats (Tabl. 2.1).

Table 2.1. — Table determine the potential threats, depending on the frequency of their manifestation

P_i	The incidence of threats
0.67	threat appears no more than once every 5 years
0.133	threat appears no more than once a year
0.2	threat appears no more than once a month
0.267	threat appears no more than once a week
0.333	threat manifests itself daily

Step 1.4 Definition of implementation of each i -th threat considering the frequency of its occurrence is under expression:

$$w_i = w_i^C P_i \cup w_i^I P_i \cup w_i^A P_i \cup w_i^{Au}, P_i = 1, \quad (2.4)$$

where $w_i^C, w_i^I, w_i^A, w_i^{Au}$ — expert weights security services: confidentiality, integrity, availability, authenticity, P_i — probability of the i -th threat.

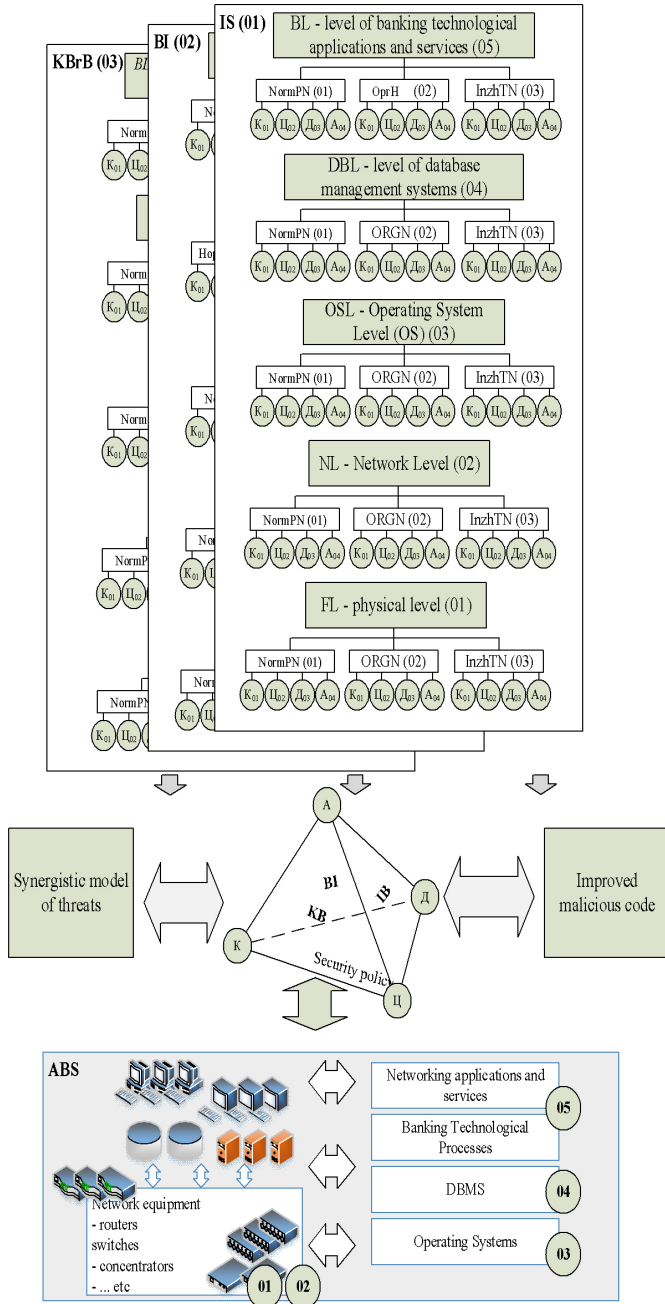


Fig. 2.6. Relationship block diagram of the classifier threats ABS OPS

Step 1.5 *Determining the likelihood of multiple threats at specified security service determined by the expression (2.4):*

$$\begin{aligned}
 W_{synerg}^C &= \sum_{i=1}^N w_i^C P_i - \text{service Privacy}; \\
 W_{synerg}^I &= \sum_{i=1}^N w_i^I P_i - \text{service integrity}; \\
 W_{synerg}^A &= \sum_{i=1}^N w_i^A P_i - \text{service availability}; \\
 W_{synerg}^{Au} &= \sum_{i=1}^N w_i^{Au} P_i - \text{the authenticity of the service},
 \end{aligned} \tag{2.5}$$

where N — total number of threats in the classifier.

In forming the metric coefficients believes that the results relate to independent threats if their relationship (coincidence classifier threats) must use the full expression determining the probability of dependent events:

$$P(AB) = P(A) + P(B) - P(AB). \tag{2.6}$$

Statistical analysis of the results of the impact assessment capabilities of i -th threats to security service experts ABS conducted by the method described in [55]. The final assessment of the i -th averages threat by the number of experts in accordance with the expression:

$$\tilde{x}_i = \frac{\sum_{n=1}^N x_n \times k_n}{N}, \tag{2.7}$$

where: x_n — grade n -th expert i -impact threat;

k_n — expert competence;

N — the number of experts.

The measure of consistency of expert opinion is considered a variance, which is calculated by the expression:

$$\sigma_x^2 = \frac{1}{N} \sum_{n=1}^N k_n (x_n - \tilde{x}_i)^2, \tag{2.8}$$

The statistical significance of the results with probability $1 - P_t$ is: $[\tilde{x}_i - \Delta, \tilde{x}_i + \Delta]$,

where the value x_i normally distributed with the center in $\tilde{x}_i$ and dispersion σ_x^2 .

Then Δ is defined by the expression:

$$\Delta = t \sqrt{\sigma_x^2 / N}, \tag{2.9}$$

where t — the quantity that obeys student distribution for $N - 1$ degrees of freedom, N — number of experts.

Step. 1.6 *Determination of the total threats for the safety components on the basis of expression (2.3) is determined by:*

$$\begin{aligned} W_{synerg}^{IB} &= \sum_{i=1}^N (w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}) P_i, \\ W_{synerg}^{KB} &= \sum_{i=1}^N (w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}) P_i, \\ W_{synerg}^{BI} &= \sum_{i=1}^N (w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}) P_i. \end{aligned} \quad (2.10)$$

Step. 1.7 *Definition of generalized synergetic threats in the BI ABS:*

$$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \cup W_{synerg}^{KB} \cup W_{synerg}^{BI}. \quad (2.11)$$

Step 1.8 *Definition of generalized synergetic threats based on their hybridity is determined by:*

$$W_{synerg}^{hybrid\ C,I,A,Au} = W_{synerg}^C \cap W_{synerg}^I \cap W_{synerg}^A \cap W_{synerg}^{Au}. \quad (2.12)$$

The research results threats max the frequency BI on their display in ABS are given in Table. 2.2.

Table 2.2. — Results threat assessment based on a synergistic approach

Safety components	Security services				Result
	C, W_{synerg}^C	I, W_{synerg}^I	A, W_{synerg}^A	A_u, W_{synerg}^{Au}	
IS, W_{synerg}^{IB}	0.023	0.223	0.193	0.207	0.0002
KB, W_{synerg}^{KB}	0.222	0.234	0.197	0.134	0.0014
BI, W_{synerg}^{BI}	0.226	0.109	0.152	0.189	0.0007
Result	0.471	0.566	0.542	0.53	
$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \cup W_{synerg}^{KB} \cup W_{synerg}^{BI} =$ $= 0.0002 + 0.0014 + 0.0007 = 0.0223$			$W_{synerg}^{hybrid\ C,I,A,Au} =$ $= W_{synerg}^C \cap W_{synerg}^I \cap W_{synerg}^A \cap W_{synerg}^{Au} =$ $= 0.471 \times 0.566 \times 0.542 \times 0.53 = 0.0766$		

Developed a software tool that implements advanced Classification of information security threats BI in ABS, which unlike the known synergistic model based threats, which allowed to classify threats by security components, types of services and infrastructure hierarchy levels of automated banking systems. Practical implementation allows on-line form expert evaluation of

threats BI, analyze synergies and hybridity, assess the likelihood of the impact of these threats to information security of banking information without significant cost investment and human resources (electronic access to the resource: <http://skl.hneu.edu.ua/>).

To determine the relationships between the elements of infrastructure ABS information assets BI, threats IS, CB, SI and TMIP in step 2, consider an improved model of infrastructure ABS synergistic model threats and improved model of the attacker.

2.3 The formalization of the problem of evaluation generalized index of banking information security in automated banking systems

2.3.1 Improving the infrastructure of automated banking system

One of the most important tasks of constructing optimal comprehensive information security system is the choice of a plurality of such means of recruitment, which will ensure neutralization of all the potential threats of information with the best quality and the lowest possible cost resources. The most effective information security problems are solved under preventive protection strategy when evaluated at the design stage potentially possible threats and implemented mechanisms to protect them. In the process of designing systems with a developer having statistics on the results of the operation created a system has to decide on the composition of a means of CO being in the face of considerable uncertainty [1, 48, 56, 59, 61].

Security models play an important role in the development and research of secure computer systems which include ABS. Models provide system integrators approach that includes addressing critical problems: choice and study the basic principles of the architecture of ABS, defining mechanisms for implementing the means and methods of information security, proof of properties (security) developed systems by formal proof of compliance with security policies (requirements, conditions, criteria) drafting formal specification of security policy as an essential component of organizational and documentation software developed protected computer systems.

Construction of models when designing or upgrading of information security in banks seems naturally solving analysis and design with minimal cost and high efficiency. Thus, the analysis stage model of information security used to study each functions (operations) to detect, for example, what information and what resources should have access to every worker on duty [1, 48, 56, 59, 61].

The main result of the formation of the methodological foundations of security BI in ABS, according to a systemic approach [57, 59, 61, 63, 64, 65, 66, 67,

70, 74] is an idealized or reference model (RM) protected ABS, realizing fundamentally safe technologies circulation BI. In addition, RM provides the potential for implementing decisions standardization and harmonization of architectural approaches, by developing regulations and standards in the security BI.

To build a security model based on a synergistic approach to threat assessment BI, regardless of component safety: IS, CB, SI appropriate to apply risk management principles, which will allow for proper use of its basic procedures promptly identify and classify threats and, according to the likelihood of negative consequences of their possible manifestations organize a system of adequate security BI in ABS.

In [1, 2, 30, 38, 39, 45, 46, 47, 48, 56, 57, 59, 60, 61, 62, 63, 64, 67, 68, 69, 70, 73] noted that security information, including banking, can be provided only in the complex the whole gamut of available remedies in all structural elements of the production system and at all stages of the cycle processing. Ignoring system analysis methodology to establish system of banking information based on the difficulty and sometimes impossibility of objective confirmation of established system efficiency due to imperfect regulatory and methodological information security, especially in the field of indicators and criteria [69, 72, 74] just creates obstacles to the solution of the abovementioned problems.

Development theories IS, CB, SI is now associated with the new circumstances specific to the modern period of development of information society based on high technology. *First*, because it is more urgent not only data protection but also protection of the community, people and communication systems primarily critical applications (CA) from the damaging effects of information in cyberspace, the emerging problem of security as an organic totality problems of information security and protection of information.

Second, from the start of regular use of automated information processing technology urgency of the task to ensure the required quality of information increases, and the problem becomes complicated. Thus, the evolution of computing technology leads to emergent properties of automated systems management and security tasks impossible without quality assurance information.

Third, problem solving information security, information protection objectives and quality of information determines the effectiveness of the projects. There is a generalized concept of information management that integrates concepts are defined above. In turn, job accounting information management required for the formation, maintenance and use of the concept of information support of the objects.

Fourthly, serious attention to the new stage of development of the theory of information security should be given to improving the scientific and meth-

odological basis and tools that ensure resolution of any emerging challenges on a regular basis in organic connection to the problems of information security, information technology, information society. So, the foregoing reveals the following most urgent problems of the theory and practice of IS [2, 36, 37, 39, 45, 48]:

- creation of theoretical bases and the formation of scientific and methodological basis that can adequately describe the processes in the face of considerable uncertainty and unpredictability manifestations of destabilizing factors (threat information) in interconnecting synergetic approach to the evaluation of all components of the concept of security, IS, CB, SI;
- develop scientifically grounded regulatory guidance documents on security BI in ABS based on the study and classification of threats to information and to develop standard requirements for protection;
- standardization of approaches to creating information security systems and streamlining management structures and circuits for protection object, regional and national levels.

Solutions range of these problems is important for the implementation of the National Security Strategy of Ukraine Doctrine and security of banking information. Obviously, one of the most important tasks of constructing optimal comprehensive information security system is the choice of a plurality of such means of recruitment, which will ensure neutralization of all the potential threats of the best quality and the lowest possible cost resources. To that end security model used, allowing to synthesize security settings ABS to reduce labor costs and increase the degree of compliance with regulations when designing systems (subsystems) CO and planning protection throughout the cycle TSZI use in ABS.

Fig. 2.7 summarizes the synergetic approach to building security model BI in ABS.

Analysis Fig. 2.7 shows that the main difference between the proposed approach simulation model of security against known is, firstly, the use of a synergistic approach to constructing a model of threats, giving emergent effect of obtaining interconnecting threat assessment BI, secondly, to ensure successful implementation of business processes with features safety BI in ABS selected items based on the requirements:

- ensuring the confidentiality of information;
- ensuring access to information, services and network and hardware subsystems;
- ensure the integrity of information;
- ensuring business continuity.

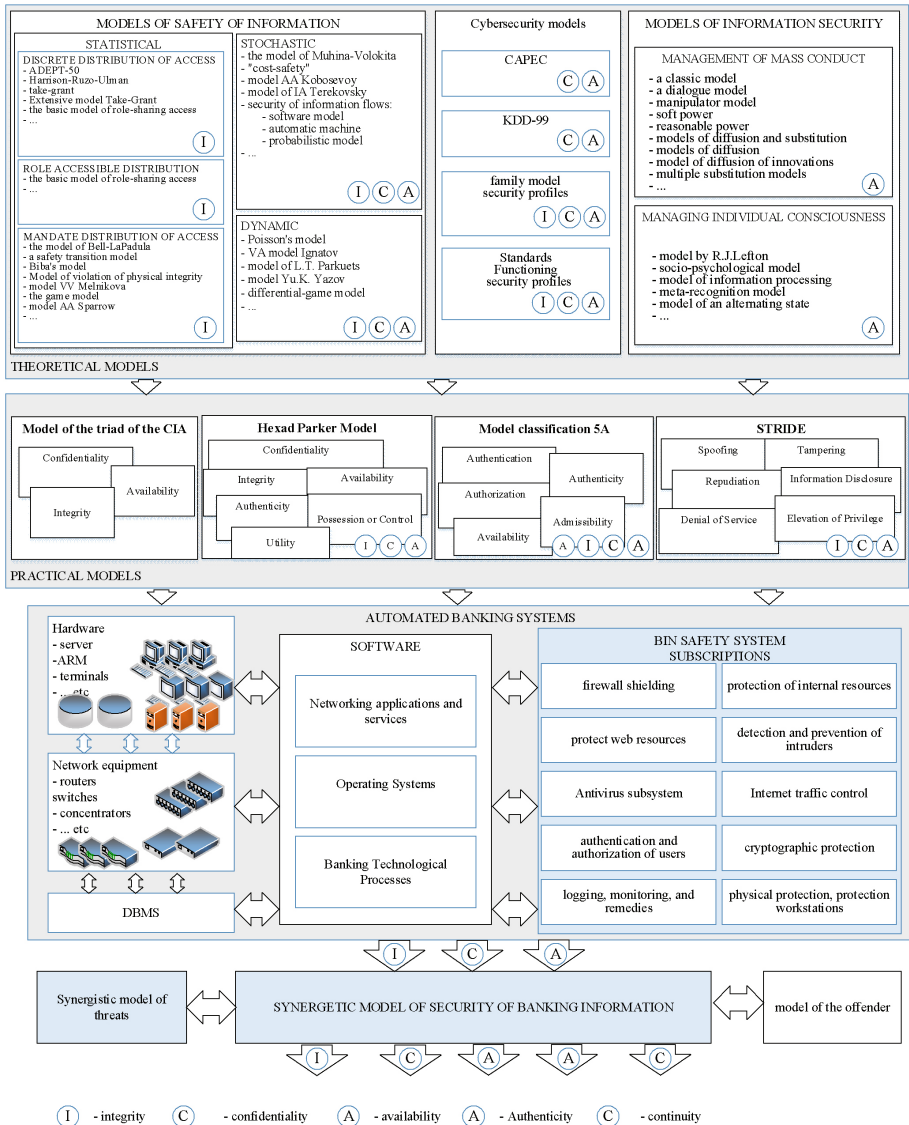


Fig. 2.7. A generalized approach of forming synergistic security model BI

In practice, the most widely used two approaches to study the draft security subsystem [1, 45, 57].

The first is based on checking the compliance of IP protection requirements of one of the standards in the field of information security. It can be a form of protection according to requirements of protection profiles developed

according to the standard ISO-15408 or any other set of requirements. Then the goal criterion in security — a given set of performance requirements. The criterion of effectiveness — the minimum total cost of fulfillment of functional requirements: $\sum c_i \rightarrow \min$, where c_i — the cost of the i -th remedy. The main drawback of this approach is that in the event that the required level of protection is not rigidly specified (e.g. through legal requirements) to determine the “most effective” protection level ABS is difficult.

The second approach to building security system linked with assessment and risk management based on the principle of “reasonable sufficiency”. However, the analysis showed that the balance between the cost of protection and the resulting effects, including and economic, that is to reduce losses from security breaches is subjective and depends on the risk assessment of threats to the elements ABS.

The analysis [1, 22, 23, 26, 34, 35, 36, 37, 41, 45, 47, 48, 52, 56, 57, 59, 60, 61, 62, 63, 64, 70, 71, 73] introduce a definition of information security, basic mechanisms and procedures as part of building a security model based on BI synergistic approach:

Definition 4. *Banking information (BI)* — the information resulting from banking activities, as well as information characterizing the bank itself, its financial position, performance and reliability requirements of the law.

Definition 5. *Privacy (confidentiality)* — BI condition in which the information can not be obtained by unauthorized users and/or processes.

Definition 6. *Privacy system (system confidentiality)* — property system to protect BI in the transfer from passive attacks;

Definition 7. *Integrity (integrity)* — BI condition in which the information can not be modified by an unauthorized user and/or process.

Definition 8. *The integrity of the system (system integrity)* — property system to protect the storage BI and BI possibility of modifying only the authorized user and/or process.

Definition 9. *Availability (availability)* — BI condition in which there are no obstacles to access to information and regular use of the authorized user and/or process.

Definition 10. *Availability of the system (system availability)* — property of the system, which is that the authorized user and/or process that has proper authority can use the resource in accordance with the rules laid PB without waiting longer given (small) amount of time, as required the user to place required the user and the time when it is needed.

Definition 11. *Authenticity (authenticity)* — BI condition in which the information provides authentication source (authorized user and/or process) of information.

Definition 12. *The authenticity of the system (system authenticity)* — property system, which is that the authorized user and/or process with relevant authority may confirm the authenticity of sources.

Definition 13. *Business continuity (Business continuity)* — property system, which is to ensure the smooth operation of the internal and external application workloads and services operate without interruption during planned downtime and unplanned disruptions and ensure backup and storage of critical business data and the possibility of their recovery within a reasonable period of time in case unexpected incident or accident.

Definition 14. *Items threats IS* — information on the composition, condition and performance of the bank (personnel, material and financial values, information resources bank).

Definition 15. *Security Threats BI* — a set of conditions and factors endangering unauthorized, including random, access to bank data, which may be the result of the destruction, modification, blocking, copying, distribution BI and other tamper with their treatment in ABS.

Threats to information expressed in violation of its availability, integrity, authentication and confidentiality.

Definition 16. *Synergetic indicator banking information security in ABS* — evaluating the effectiveness of synergetic integrated application capabilities banking information security in terms of antagonistic counteraction system of bank protection random and targeted security threats.

A threat act competitors, criminals, hackers and insiders. Sources of threats while pursuing the following objectives: familiarization with banking information in their modification and destruction of useful purposes for the application of direct material losses.

Illegal appropriation of confidential information is possible due to its disclosure, leakage BI through technical means and unauthorized access to the BI.

Sources staff is confidential information, bank processes, documents, technical media BI, means providing banking transactions.

The main areas of information security is a legal, organizational and technical protection of information as exponents of an integrated approach to information security BI.

Remedies information is physical, hardware, firmware, and cryptographic methods. As a means of protection serve organizational and technical measures, methods and steps to ensure prevention of illegal actions, prevention, suppression and combating unauthorized access to BI.

In summary, the components are considered as conceptual synergetic security model BI in Fig. 2.8.

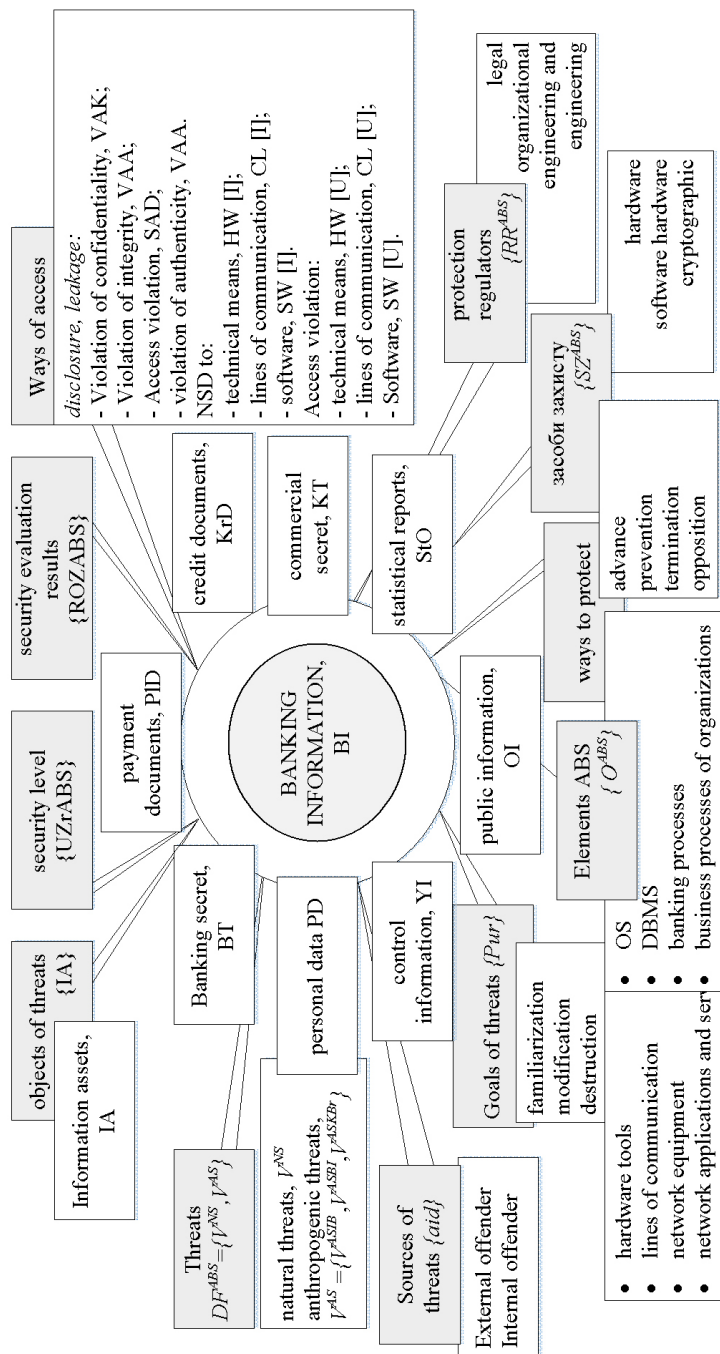


Fig. 2.8. Conceptual block diagram synergetic security model BI

Step 2. *Defining relationships between elements of infrastructure ABS information assets BI, threats IS, CB, SI and TMIP improved model based infrastructure ABS synergetic model threats, improved model of the attacker.*

Conceptual synergistic security model BI is based on the methodology and synergetic approach to security BI and evaluation of the security BI ABS Ukraine under hybridization threats to the components of security: IS, CB, SI in a BI in ABS and private models: improved infrastructure models ABS synergetic model threats and improved model of offender assessment model protection ABS.

Infrastructure ABS model is the next formal model:

$$G^{ABS} = \{ \{O^{ABS}\}, \{L^{ABS}\}, \{I_A\} \}, \quad (2.13)$$

where:

O^{ABS} — set of objects environment, describing elements of ABS and they belong to levels of hierarchy ABS;

L^{ABS} — set of relationships between elements, determined adjacency matrix:

$$A^{ABS} = \|a_{ij}^{ABS}\|. \quad (2.14)$$

$\{I_A\}$ — the set of elements of information assets. Each element $I_{A_i} \in \{I_A\}$ described vector $I_{A_i} = (Type, A^C, A^D, A^A, A^K, C_Y)$. *Type* — the type of information assets, described by the set of basic values $Type = \{BT, PID, CrD, KT, StO, Ol, YI, PD\}$, where *BT* — bank secrecy, *PID* — vouchers, *CrD* — credit instruments, *KT* — trade secrets, *StO* — statistical reports, *Ol* — public information, *YI* — managing information, *PD* — personal data, A^K — confidentiality, A^C — integrity, A^D — availability, A^A — authenticity, C_Y — continuity — the properties of information that must be provided. Takes values 1 — if the property is necessary, 0 — otherwise.

Step 2.1 *Determining the link between information assets BI $\{I_A\}$ and elements of infrastructure ABS $A^{ABS} = \|a_{ij}^{ABS}\|$. Each element $I_{A_i} \in \{I_A\}$ described vector $I_{A_i} = (Type, A^C, A^I, A^A, A^{Au}, C_Y)$, *Type* — the type of information assets, described by the set of basic values $Type = \{BT, PID, CrD, KT, StO, Ol, YI, PD\}$, where *BT* — bank secrecy, *PID* — vouchers, *CrD* — credit instruments, *KT* — Commercial mystery, *StO* — statistical reports, *Ol* — public information, *YI* — control information, *PD* — personal data, A^C — confidentiality, A^I — integrity, A^A — availability, A^{Au} — authenticity, C_Y — continuity — the properties of information that must be provided. Takes values 1 — if the property is necessary, 0 — otherwise.*

Step 2.2 *Determine connection between information assets $\{I_A\}$ objects and environment.* Each element $O_i \in \{O^{ABS}\}$ described vector $O_i = \{Y^{ABS}, IO\}$ where Y^{ABS} — level hierarchy information structure, defined by a plurality $Y^{ABS} = \{FL, NL, OSL, DBL, BL\}$, where FL — physical layer, NL — network level, OSL — level operating systems (OS), DBL — level systems database management, BL — level banking technology applications and services. To specify the connection type and IO^R existing relationship between information assets and real environment using generally used:

$$IO^R = \|IO_{il}^R\|, \quad (2.15)$$

where IO_{il}^R — reflects the presence and type of connection between the i -th information assets and l -object of protection ABS. With $\forall i \in \{I_A\}$, a $\forall l \in \{O^{ABS}\}$:

$$IO_{il}^R = \begin{cases} 0, \text{connection is absent} \\ cs, \text{include and save} \\ pt, \text{processes and transmits} \\ so, \text{supports operation} \end{cases} \quad (2.16)$$

The next step — defining a plurality of integration based threats synergetic model threats and generalized model of the offender.

2.3.2 Development of a conceptual model of synergistic threats to information security of banking information in automated banking systems

Step. 2.3 *Definition of integration sets threats based threats synergetic model and generalized model of the offender.*

Synergetic Model threats formally described by:

$$GR^{ABS} = \{\{DF^{ABS}\}, \{T_{risk}\}, \{T_p\}, \{T_U\}, \{VH\}\}. \quad (2.17)$$

A plurality of sources of security threats presented ABS tuples:

$$DF^{ABS} = \{V^{NS}, V^{AS}\},$$

in which: V^{NS} — class natural sources of threats;

$$V^{AS} = \{V^{ASIB}, V^{ASKB}, V^{ASBI}\} \text{ — class anthropogenic threats where:}$$

V^{ASIB} — set of information security threats, V^{ASKV} — set of cyber security threats, V^{ASBI} — set of information security threats. T_{risk} — qualitative indicator of risk, T_p — set of basic terms probability of at least one threat j -th asset, T_U — set basic terms the value of the loss from the sale of threats ui , VH — set a destructive state of elements of ABS, which refers to unwanted and unplanned state of the component ABS, in which he found himself as a result of one or more threats.

For synergies enhance the security BI must consider integration of threats:

$$DF^{ABS} = \{V^{NS}\} \cup \{V^{AS}\}, \quad (2.18)$$

where $\{V^{AS}\} = \{V^{ASBI}\} \cap \{V^{ASIB}\} \cap \{V^{ASKB}\}$.

Each element of the plurality of threats $DF_i \in \{DF^{ABS}\}$ may be represented by the following vector value $DF_i(p, u, risk)$, where p — the probability of threats, u — potential loss, $risk$ — the risk is expressed in a qualitative manner and adopting one of two states $T_{risk} = \{\text{valid, invalid}\} = \{\alpha_{r1}, \alpha_{r2}\}$.

Step 2.4 *Definition full price of risk assets BI. Price risk is the full amount of the price of risk assets:*

$$R_{full} = \sum_{j=1}^n R_j. \quad (2.19)$$

Step 2.5 *Determining the probability of at least one threat to each asset BI.* Calculation of the probability of at least one threat for each asset is performed by the expression:

$$p_{rj} = 1 - \prod_{i=1}^m (1 - pr_{ij}), \quad (2.20)$$

where p_{rj} — probability of realization of at least one threat j -th asset.

It is assumed that in the case of for j -th asset in at least one of the plurality of threats $V^{AS} = \{V^{ASIB}, V^{ASBI}, V^{ASKBr}\}$ damage is asset-based asset detail and careful selection of current threats:

$$q_j = u_j. \quad (2.21)$$

It is believed that the threat can be implemented independently of each other [72], Then the price risk R_j for each j -th asset is determined by the expression:

$$R_j = pr_j \times q_j. \quad (2.22)$$

Thus, the probability of realization pr_j environment, with the area determine $R = [0, 1]$ ask according to [73] set basic terms $Tr = \{\text{unrealized, minimum, medium, high, critical}\} = \{\alpha_{x1}, \alpha_{x2}, \alpha_{x3}, \alpha_{x4}, \alpha_{x5}\}$.

Evaluation of potential losses from the sale of threats is closely linked with the capital (see Expression (2.18)) and is based on expert opinion. The value of the loss from the sale of threats ui given set of basic terms $T_u = \{\text{Minimum, medium, high, critical}\} = \{\alpha_{y1}, \alpha_{y2}, \alpha_{y3}, \alpha_{y4}, \alpha_{y5}\}$. To switch between qualitative and quantitative values using generally proposed in [73].

To determine the value of risk we use the rule proposed in [70] on the basis of unclear statements, expression (2.23):

$$\tilde{L} = \begin{cases} \tilde{L}_1 : \langle E_{11} \cup E_{12} \cup E_{13} \cup E_{14} \cup E_{21} \cup E_{22} \cup E_{23} \cup E_{31} \cup E_{32} : risk_i \text{ is } \alpha_{r1} \rangle \\ \tilde{L}_2 : \langle E_{24} \cup E_{33} \cup E_{34} \cup E_{42} \cup E_{43} \cup E_{44} \cup E_{51} \cup E_{52} \cup E_{53} \cup E_{54} : risk_i \text{ is } \alpha_{r2} \rangle \end{cases}$$

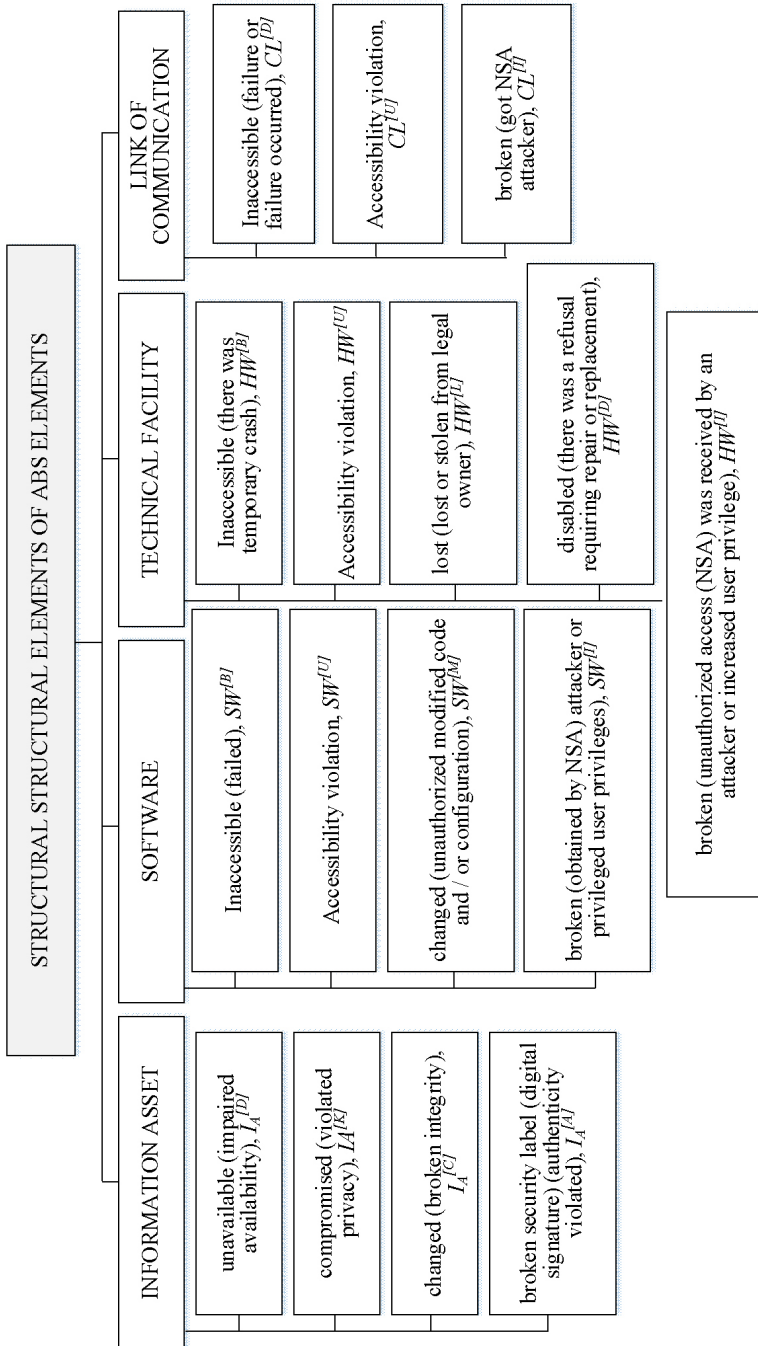


Fig. 2.9. Destructive state infrastructure ABS

Where E_{kj} : " $p_{ri} \in \alpha_{xk}$ and $u_i \in \alpha_{yj}$ ".

The analysis of documents on modeling threats, risk and reliability theory, the following states destructive elements ABS (plural $\{VH\}$, Fig. 2.9):

a) information assets:

- unavailable (broken availability), $I_A^{[D]}$;
- compromised (broken confidentiality), $I_A^{[K]}$;
- changed (broken integrity), $I_A^{[C]}$;
- broken safety label (digital signature) (broken authenticity), $I_A^{[A]}$.

b) software:

- inaccessible (failed), $SW^{[B]}$;
- compromised (hacked (GCD) or an attacker elevated privileges user), $SW^{[I]}$;
- violation of accessibility, $SW^{[U]}$;
- changed (unauthorized modified code and/or configuration), $SW^{[M]}$.

c) technical means:

- not available (there was a temporary disruption), $HW^{[B]}$;
- violation availability, $HW^{[U]}$;
- unable to work (there was a failure, requiring repair or replacement), $HW^{[D]}$;
- lost (there was a loss or theft of the legitimate owner), $HW^{[L]}$;
- compromised (hacked (GCD) or an attacker elevated privileges user), $HW^{[I]}$.

d) link:

- unavailable (failed or failure), $CL^{[D]}$;
- violation availability, $CL^{[U]}$;
- compromised (NCC received attacker), $CL^{[I]}$.

The next section is considered advanced model of the offender.

2.3.3 Improving the offending model based on a synergistic approach to the assessment of threats to information security, cyber security, and information security

One of the main threats of the model is a model of the offender that provides semantic relations between a full description of the threats and opportunities the assumption of wrongdoing, which is the source of the threats, which he can use to design and conduct attacks, as well as restrictions on these opportunities.

To construct the model used by the intruder approaches, with common classification criteria, but not always correlated to different sources.

When building models offender allocate internal and external perpetrators and take into account [47, 58]:

- presence of offenders accessing standard means (a set of software, hardware-software and hardware);
- knowledge of the targets offenders;
- the level of training violators;
- the use of various means offenders for the attack;
- pursued violators purpose;
- the possible collusion different categories of offenders.

In addition to these aspects, the construction of models in ABS offender should be considered for matching objects access of attacks, channel description attacks, attacks justify exclusion of subjects with the number of potential offenders, as well as life cycle and levels of ABS, which may affect the offender.

Guaranteed to meet the challenges of information security in the ABS [47, 48] should take into account such offenders exposure levels: levels of technical channels, unauthorized, harmful effects, embedded devices, information security system. Established tools, which you can use with unauthorized access, can be very different: software, hardware and software and maintenance of computer technology (Sot) or ABS. It is therefore necessary to categorize the level of unauthorized access to the BI, as well as objects and lines (LS) ABS. Based on the model proposed qualifying offender characteristics define five categories (Fig. 2.10):

Category 1. Users ABS and applications — OPS employees that have opportunities for access to confidential information as part of their duties. Can influence the level of database management systems (04), and the level of banking technology applications and services (05), in order to steal information or affirmation accident.

This use technical means to intercept (TMI) without modifying the components of ABS and standard means of protection and disadvantages to overcome.

Category of users ABS advisable to divide into the following groups in terms of trust 1.1 — trusted users (e.g. top management of the organization BS); 1.2. — user (most workers OPS); 1.3 — user “at risk” (e.g. OPS employees on probation who applied for release or previously involved in incidents IS).

Category 2. Operating personnel — persons, including non-employees BS organization, have opportunities to access information of a confidential nature in carrying out tasks related to the operation and (or) administration of information infrastructure OPS, ABS and applications organization BS. Can affect all levels — physical layer (01), network layer (02), the level of operating systems (OS) (03), the level of database management systems (04), the level of banking technology applications and services (05), in order to steal

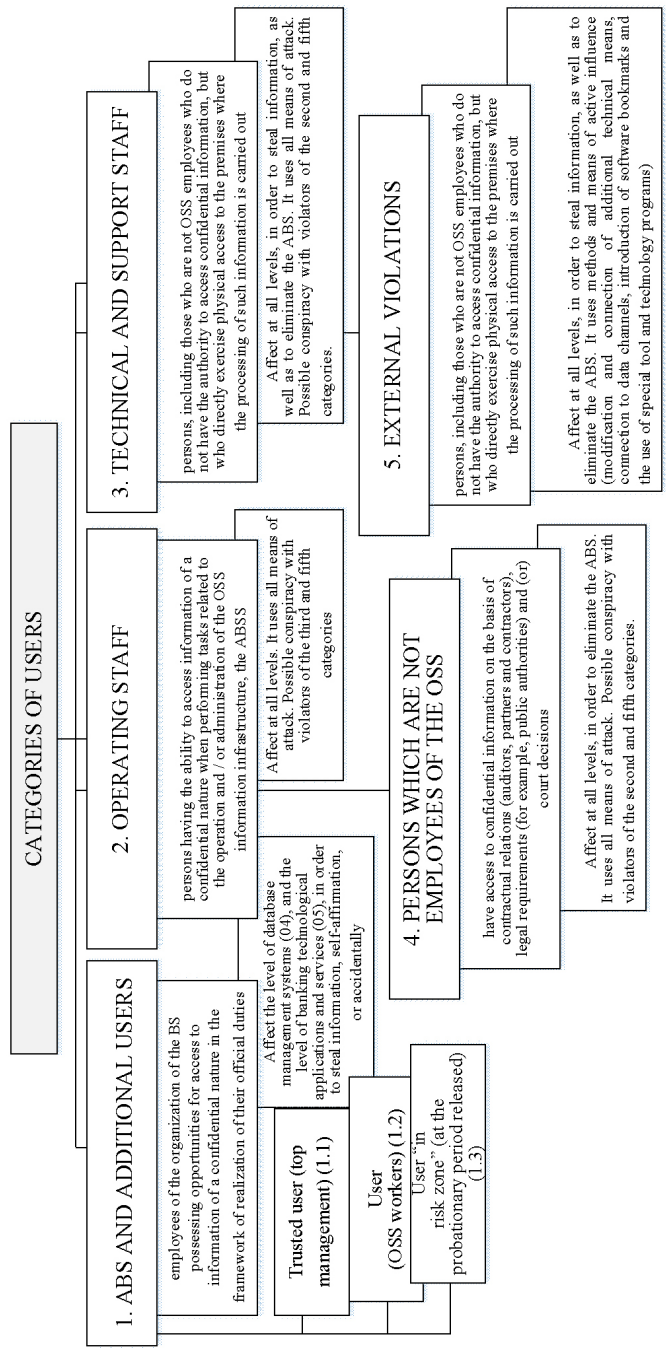


Fig. 2.10. The classification of offenders in ABS

information and to disable the ABS. This means using all attacks. Possible plot against violators third and fifth categories. Do not have access rights to the network configuration of means, except for control (inspection).

Category 3. Technical and support staff — persons, including non-employees OPS that do not have powers of access to confidential information, but perform direct physical access to the premises in which the processing of such information. Can affect all levels physical layer (01), network layer (02), the level of operating systems (OS) (03), the level of database management systems (04), the level of banking technology applications and services (05), in order to steal information and to disable the ABS. This means using all attacks. Possible plot against violators of the second and fifth categories.

Category 4. Persons who are not employees of the organization BS, have access to confidential information on the basis of the contractual relationship (such as auditors, partners and contractors) legal requirements (e.g. public authorities) and (or) the judgment. Can affect all levels, in order to disable the ABS. This means using all attacks. Possible plot against violators of the second and fifth categories. Do not have access to the information security and logging and key elements of the ABS.

Category 5. External offenders, which are persons engaged influence outside the controlled zone OPS. Can affect all levels in order to steal information, assertiveness and disable the ABS. This use methods and means of active influence (modification and connection of additional technical means connecting to data channels, bookmarks and implementation of software using special tools and technology programs).

This classification covers aspects more fully reflected in regulatory guidance documents, and enables uniquely classify the offender.

Formal models offender define the propositions authors [58, 68]:

$$G_{IA}^{ABS} = \{aid_i, pur_i, T_{IA}, S_{\max_i}, pr_j, MS_i^{ABS}\} \forall i \in n, \forall j \in m, \quad (2.24)$$

where $aid_i \in \{aid\}$ — ID offender (violation category), $pur_i \in \{pur_i\}$ — the purpose of the offender, T_{IA} — a successful implementation of threats, $S_{\max_i}$ — probabilistic damage system, $MS_i^{ABS} = \{ms_i\}_{i=1}^{N_{MS^{ABS}}}$ — recommendations on detection, response TMIP, $N_{MS^{ABS}}$ — the number of recommendations known ABS, n — number of threats, m — number of assets.

A plurality of sources of threats includes four types of sources:

$$DF^{ABS} = \{V^{NS}, V^{AS}, TS, PI, NI\}, \quad (2.25)$$

where DF^{ABS} – set of sources of security threats ABS, which V^{NS} – class natural sources of threats $V^{AS} = \{V^{ASIB}, V^{ASBI}, V^{ASKB}\}$ – class anthropogenic threats where V^{ASIB} – set of threats to information security, V^{ASBI} – set of threats BI, V^{ASKB} – set of threats CB; TS – hardware and systems; PI – intentional violators; NI – unintentional offenders (criminals).

Emission of threats called one or more passages related components in ABS destructive conditions from exposure to sources of threats. One or more scenarios of threats can be represented by directed graph $G(V, H)$, wherein: the initial peak (v_0) is set, one of the species or specific source of threats; intermediate and final vertices (v_n) is a destructive state of ABS components; arcs (h_{ij}) unite two peaks, one of which is the cause (v_i), and the second – the result and the result of the transition (v_j), scenario implement privacy threats considered in [74].

To assess the degree of hazard indicators offenders and the degree of implementation of protective measures define sets of weighted metrics that take values in the range $[0, 1]$. Each metric describes a certain extent to the offending signs or protective measure given target value.

To assess the degree of danger the offender is proposed to use the following metrics formed with the provisions [72, 75]: Motivation equipped (existing equipment), technical expertise, knowledge and information about ABS TSZI, permissions (to implement threats), access (to the discovery and response degree of danger of i-offender is defined by the expression:

$$d_i = \Pi \left(M_{ih}^{DF^{ABS}} \right)^{w_{ih}^{DF^{ABS}}}, \quad (2.26)$$

where $M_{ih}^{DF^{ABS}}$ – the value of h -oh metric of i -offender;

$w_{ih}^{DF^{ABS}}$ – weighting metrics h -oh i -th offender $\sum_h w_{ih}^{DF^{ABS}} = 1$.

Metrics degree of implementation of protective measures, which are divided into preventive (preventing switching element in the ABS destructive state) ψ_j and adjusting (reducing the value of loss on conversion) ψ'_j define the expression:

$$\psi_j = \Pi \left(\sum_g w_{gl}^{SZ^{ABS}} \times M_{gl}^{SZ^{ABS}} \right)^{w_{jg}^K}, \quad (2.27)$$

where: $M_{gl}^{SZ^{ABS}}$ – l -value metric oh safeguard measure g -category;

$w_{gl}^{SZ^{ABS}}$ – weight l -oh safeguard measure g -category, $\sum_l w_{gl}^{SZ^{ABS}} = 1$;

w_{jg}^K – g -weight category, $\sum_g w_{jg}^K = 1$.

The degree of implementation of corrective safeguard measures ψ'_j similar to ψ_j given by (2.27).

Vector weighting coefficients W is determined by the valuation resulting vector priorities determined by an expert:

$$w_i = \frac{\bar{b}_i}{\sum_{i=1}^m \bar{b}_i}, \forall i \in [1; m], \bar{b}_i = KE \sqrt{\prod_k b_{ik}}, \quad (2.28)$$

where $\bar{b}_i$ — the resulting priority of the i -th element, b_{ik} — i -priority element, rated k -th expert, m — dimension matrix of pairwise comparisons, KE — number of experts.

Formation of the expert group (number of experts) to calculate the formula that proposed in [55]:

$$K \geq 0.5(0.33 / \beta + 5), \quad (2.29)$$

where β — error results of expert analysis or acceptable probability of error.

Consistency of the estimates determined twice [74]. Initially estimated index of consistency guest expert:

$$C_E = \frac{\lambda_{k_{\max}} - m}{m - 1}, \quad (2.30)$$

where $\lambda_{k_{\max}}$ — the maximum amount of own matrix of pairwise comparisons k -th expert; m — dimension matrix of pairwise comparisons.

Experts estimate considered consistent if the consistency ratio $CR = CE / CIS$, where the CIS — the average consistency index, defined as the range (tab. 2.3).

Table 2.3. — CIS and CR values of m

m	3	4	5	6	7	8	9	10	11	12
CIS	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49	1.51	1.48
CR	[0; 0.05]	[0; 0.08]	[0; 0.1]							

Consistency opinions of the expert group is determined by three sigma rule. inconsistent estimates are not included in the calculation of the resulting vector priorities $\bar{B} = (\bar{b}_1, \bar{b}_2, \dots, \bar{b}_m)^T$.

Confidence interval δ_i is given by:

$$\delta_i = t_{cm} \times \sigma_{gi} / \sqrt{K}, \quad (2.31)$$

where $t_{st} = 0.95$ — Student test;

Step 2.6 *Determining the link between the sources of threats and elements ABS:*

$$A^{DF} = \|a_{ij}^{DF}\|. \quad (2.32)$$

The next step is to determine the generalized index of IS BI in ABS based on the improved model of evaluation of the security BI in ABS.

2.3.4 Improving evaluation model of banking security in automated banking systems.

Step 3. Definition of generalized index of IS BI in ABS based on improved model of evaluation of the security BI in ABS.

Definition of security threats ABS IS, CB, SI BI on the ABS invited to get through improved model of banking information security in automated banking systems:

$$G_{OZ}^{ABS} = \left\{ \left\{ I_A \right\}, \left\{ O^{ABS} \right\}, \left\{ DF^{ABS} \right\}, \left\{ RR^{ABS} \right\}, \left\{ SZ^{ABS} \right\}, \left\{ ROZ^{ABS} \right\}, \left\{ UZ_r^{ABS} \right\} \right\}, \quad (2.33)$$

where $\{I_A\}$ — the set of elements of information assets;

$\{O^{ABS}\}$ — set elements hierarchy ABS;

$\{DF^{ABS}\}$ — set of sources of security threats ABS;

$\{RR^{ABS}\}$ — set requirements for security controls BI;

$\{SZ^{ABS}\}$ — set TSZI possible;

$\{ROZ^{ABS}\}$ — accounting data on the results of security evaluations ABS;

$\{UZ_r^{ABS}\}$ — the level of security of ABS.

Step 3.1 determining the link between threats and means of information security (TMIP):

$$A^{DFSZ} = \left\| a_{ij}^{DFSZ} \right\|, \quad (2.34)$$

with $\forall j \in \{I_A\}$, and $\forall i \in \{DF_i\}$.

$$\left\| A^{DF} \right\| = \begin{cases} 1, & \text{if there are } i\text{-threats to the } j\text{-th asset,} \\ 0, & \text{if there are no } i\text{-threats to the } j\text{-th asset.} \end{cases} \quad (2.35)$$

Each protection mechanism BI in ABS $SZ_i \in \{SZ^{ABS}\}$ characterized by the vector $SZ_i = (T_{SZ}, T_V, C_{SZ})$ where T_{SZ} — type of remedy, T_V — the implementation, C_{SZ} — cost.

To describe the connection between the threats and TMIP matrix is used:

$$A^{DFSZ} = \left\| a_{ij}^{DFSZ} \right\|, \quad (2.36)$$

where a_{ij}^{DFSZ} — reflects the link between i -th security threats caused

$DF_i \in \{DF^{ABS}\}$ and j -th TMIP $SZ_i \in \{SZ^{ABS}\}$.

The model used the following types of communication: MZ — is a defense mechanism that provides the opposition to its destructive influence $VH_i \in \{VH\}$; NMZ — no protection mechanism to ensure the i -th counter threats.

With $a_{ij}^{DFSZ} \in \{MZ, NMZ\}$, MZ , NMZ — the link between a certain type of i -th and j -threat of TSZI. For values of matrix elements defined by the rule:

$$\left\| a_{ij}^{DFSZ} \right\| = \begin{cases} MZ, & \text{if } i\text{-th threat is disclosed } j\text{-th TZZI;} \\ NMZ, & \text{if } j\text{-th threat is disclosed } j\text{-th TZZI.} \end{cases} \quad (2.37)$$

If all $i = m$ $a_{mj}^{DFSZ} = NMZ$, then concludes that TMIP ABS can not protect

Bing from this destructive influence and thus to increase the level of security of ABS must raise additional funds for protection mechanisms.

Step 3.2 *Defining the requirements of regulators* $\{RR^{ABS}\}$ that includes requirements for security BI — $\{R_{BBI}\}$, defined in international and national standards set estimates the extent to which safety requirements $\{OV_{BBI}\}$ and set the final level of compliance with the safety requirements set BI $\{IU_{BBI}\}$:

$$\{RR^{ABS}\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}. \quad (2.38)$$

Step 3.3 *Definition of generalized index of security of ABS, which allows you to assess the level of compliance and regulatory requirements TMIP determined:*

$$OPZ^{ABS} = \sum_{i=1}^k OPZ_i, \quad (2.39)$$

where: k — number of individual safety parameters,

OPZ_i — index takes the value from the set:

OPZ_1 — the absence of unacceptable risk, if in OPS threats in the preparation of model/models offender and found unacceptable risk to the level of risk is $OPZ_1 = 0$, otherwise — $OPZ_1 = 1$;

OPZ_2 — no dangerous threats closure mechanisms TMIP, $OPZ_2 = 0$, if the OPS in the preparation of a model found “unbalanced” threat — $OPZ_2 = 1$;

OPZ_3 — level security compliance requirements BI regulators recommended recognized — $OPZ_3 = 1$, if deemed unauthorized — $OPZ_3 = 0$.

Based on these data the system is assigned to one of three levels of security $UZ^{ABS} = \{\text{low, medium, high}\}$ according to the rules:

$$UZ^{ABS} = \begin{cases} \text{high, if } OPZ^{ABS} = 3; \\ \text{medium, if } 1 \leq OPZ^{ABS} \leq 3; \\ \text{small, if } OPZ^{ABS} = 0. \end{cases} \quad (2.40)$$

The resulting audit assessment of the security BI to determine the most valuable information assets BI, the effectiveness of the means to protect them, and the degree of conformity of TMIP OPS requirements for protection and the level of security controls, identify the most vulnerable places and make recommendations to improve, if necessary, protection ABS OPS.

To assess the economic feasibility of the introduction of a mechanism to TMIP ABS OPS depending on the value of the ABS BI introduce the following notation:

$V_{BI n}^{ABS}$ — BI value for OPS (parties have the information and try to defend it)

$V_{BI n}^{IA}$ — BI value for the attacking side (which is trying to get information);

SZ^{ABS} — TMIP means possible;

$SV^{AS} = \{SV^{ASIB}, SV^{ASBI}, SV^{ASKB}\}$ — the means allocated for the ex-

traction of BI:

SV^{ASIB} — fracture mechanisms and tools TMIP IS in ABS;

SV^{ASBI} — means breaking mechanisms and TMIP SI in ABS;

SV^{ASKB} — hacking tools and mechanisms TMIP BC:

$$SV^{AS} = \{SV^{ASIB}\} \cap \{SV^{ASBI}\} \cap \{SV^{ASKB}\}. \quad (2.41)$$

The obvious fact is recognized that pointless to invest in mining or protection than the value BI:

$$SZ^{ABS} \leq V_{BI n}^{ABS}, SV^{AS} \leq V_{BI n}^{ABS}. \quad (2.42)$$

Suppose the probability determined by the expression:

$$p_{Zj} = \frac{q_Z \times SZ^{ABS}}{q_Z \times SZ^{ABS} + q_V \times SV^{AS}}; \quad (2.43)$$

$$p_{Vj} = \frac{q_V \times SV^{AS}}{q_V \times SV^{AS} + q_Z \times SZ^{ABS}}; \quad (2.44)$$

where: q_Z, q_V — weights that determine how each side close to the target;

P_{vj} — the likelihood of the realization of at least one i -th threat j -th asset (probability of success attacking side);

p_{zj} — likely to protect against the threat of the i -th j -th asset (probability of success defending side).

Assume that the amount of funds allocated to the attacking side is the value BI and BI value is the same for both sides, and opposing sides are equal, then the economic value of spending on defense BI must not exceed:

$$SZ^{ABS} = V_{BI}^{ABS} \times \frac{\sqrt{5}-1}{2}. \quad (2.45)$$

The effectiveness of the proposed model estimates the economic costs depends on the accuracy of the wording probability of success of protection and determine the value BI.

2.4 Conclusions of the second section

Thus, in the second section of the proposed concept, based on a synergetic approach to the selection of the most effective ways achieving goals IS BI in ABS to the value of risk at every level model of strategic management of the bank. As a result, the following scientific and practical results:

1. The concept of building a synergetic model of threats IS BI in ABS, basis of which is a three-tier security model of strategic management of banking information technologies. The concept covers all main areas of the bank's activities to ensure information security, based on a synergetic approach to the selection of the most effective ways achieving goals IS BI in ABS to the value of risk at every level model of strategic management of the bank and provides effective control over the implementation of ISMS functions OPS.

2. A software tool that implements advanced classification of banking information security threats in automated banking systems, which in contrast to the known synergistic model based threats, which allowed to classify threats by security components, types of services and infrastructure hierarchy levels of automated banking systems. Practical implementation allows on-line form expert evaluation of threats BI, analyze synergies and hybridity, assess the likelihood of the impact of these threats to information security of banking information without significant cost investment and human resources (electronic access to the resource: <http://skl.hneu.edu.ua>).

3. A practical method for evaluation of information security in the banking information ABS synergetic model based threats generalized model of offender assessment model security BI in ABS and ABS models of infrastructure to optimize the cost of funds for the construction of a system for IS BI in ABS. The practical significance is the ability to timely evaluation of the relationships between assets BI, infrastructure elements ABS, ABS TMIP and possible signs of threats IS, CB, IS, which allows time to adjust the guidelines of the bank of IS, plan investment in TMIP, generate preventive measures to prevention of threats.

References in Chapter 2

1. *R. Hryshchuk, and S. Yevseiev* The synergetic approach for providing bank information security: the problem formulation//Bezopasnost' informatsii, № 22 (1), p. 64–74, 2016.
2. *R. V. Grishchuk, Yu. G. Danik* Osnovy kiberbezopasnosti/ed. by prof. Yu. G. Danika. – Zhitomir: ZHNAEU, 2016.
3. *L. Sun, R. P. Srivastava, and T. J. Mock* An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions//Journal of Management Information Systems, Vol. 22, p. 3–28, 2006.
4. *A. V. Potiy, D. Yu. Pilipenko* Kontseptsiya strategicheskogo upravleniya informatsionnoy bezopasnost'yu//Radioelektronnye i komp'yuternye sistemy, № 6 (47), p. 53–58, 2010.
5. *A. V. Potiy, D. Yu. Pilipenko* Klassifikatsiya pokazateley bezopasnosti informatsii//Sistemy obrabotki informatsii, Ed. 3(84), p. 53–56, 2010.
6. *I. D. Gorbenko, A. V. Potiy, P. I. Tereshchenko* Kriterii i metodologiya otsenki bezopasnosti informatsionnykh tekhnologiy. URL: <http://www.bezpeka.com/ru/lib/spec/infosys/art108.html>. Accessed on: 7.12.2017.
7. Trusted Computer Systems Evaluation criteria, US DoD 5200.28-STD, 1985. URL: <https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf>. Accessed on: 7.12.2017.
8. Information Technology Security Evaluation Criteria, v. 1.2. Office for Official publications of the European Communities, 1991. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile. Accessed on: 7.12.2017.
9. Canadian Trusted Computer Product Evaluation Criteria, v. 3.0. Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993. URL: <http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=&index=alt&srchtxt=CANADIAN%20TRUSTED%20COMPUTER%20PRODUCT%20EVALUATION%20CRITERIA>. Accessed on: 7.12.2017.
10. Federal Criteria for Information Technology security. – NIST, NSA, US Government, 1993. URL: <https://www.commoncriteriaportal.org/files/ccfiles/ccpart1v2.3.pdf>. Accessed on: 7.12.2017.
11. ISO/IEC 15408–1:1999 – Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. URL: <https://www.iso.org/ru/standard/27632.html>. Accessed on: 7.12.2017.

12. ISO/IEC 15408–2:2005 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. URL: <https://www.iso.org/ru/standard/40613.html>. Accessed on: 7.12.2017.
13. ISO/IEC 15408–3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. URL: <https://www.iso.org/ru/standard/46413.html>. Accessed on: 7.12.2017.
14. DSTU ISO/IEC TR 13335–1: 2003 Informatsionnye tekhnologii. Rukovodstvo po upravleniyu bezopasnost'yu informatsionnykh tekhnologiy. Part 1. Kontseptsii i modeli bezopasnosti informatsionnykh tekhnologiy. URL: <http://lindex.net.ua/ua/shop/bibl/500/doc/11423>.
15. DSTU ISO/IEC TR 13335–2: 2003 Informatsionnye tekhnologii. Part 2. Rukovodstvo po upravleniyu bezopasnost'yu informatsionnykh tekhnologiy. URL: <http://www.premier-hs.com.ua/ru/content/dstu-isoiec-tr-13335-22003-nas-tanovi-z-kieruvannia-biezpiekoiu-informatsiinikh-tiekhnologhii>. Accessed on: 7.12.2017.
16. DSTU ISO/IEC TR 13335–3: 2003 Informatsionnye tekhnologii. Rukovodstvo po upravleniyu bezopasnost'yu informatsionnykh tekhnologiy. Part 3. Metody upravleniya zashchitoy informatsionnykh tekhnologiy. URL: <http://lindex.net.ua/ua/shop/bibl/500/doc/11425>. Accessed on: 7.12.2017.
17. DSTU ISO/IEC TR 13335–4: 2005 Informatsionnye tekhnologii. Rukovodstvo po upravleniyu bezopasnost'yu informatsionnykh tekhnologiy. Part 4. Vybory sredstv zashchity. URL: <http://metrology.com.ua/download/iso-iec-oh-sas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005>. Accessed on: 7.12.2017.
18. DSTU ISO/IEC TR 13335–5: 2005 Informatsionnye tekhnologii. Rukovodstvo po upravleniyu bezopasnost'yu informatsionnykh tekhnologiy. Part 5. Rukovodstvo po upravleniyu setevoy bezopasnost'yu. URL: <http://lindex.net.ua/ua/shop/bibl/500/doc/11427>. Accessed on: 7.12.2017.
19. ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements. URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534. Accessed on: 7.12.2017.
20. ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls. URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533. Accessed on: 7.12.2017.
21. ISO/IEC 27006:2015 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems URL: <http://www.iso.org/iso/home/search>.

- htm?qt=ISO%2FIEC+27006%3A2015+&sort=rel&type=simple&published=on. Accessed on: 7.12.2017.
22. Standart Ukrainy SOU N NBU 65.1 SUIB 1.0: 2010. Metody zashchity v bankovskoy deyatelnosti. Sistema upravleniya informatsionnoy bezopasnost'yu. Trebovaniya (ISO/IEC 27001:2005, MOD). URL: <https://ky-ianyn.files.wordpress.com/2010/12/nbu-27001.pdf>. Accessed on: 7.12.2017.
 23. Standart Ukrainy SOU N NBU 65.1 SUIB 1.0: 2010. Informatsionnye tekhnologii. Metody zashchity. Pravila dlya upravleniya informatsionnoy bezopasnost'yu (ISO/IEC 27002:2005, MOD) URL: <http://s-byte.com/useful/27002.pdf>. Accessed on: 7.12.2017.
 24. CEM-97/017. Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model.
 25. *D. P. Zegzhda, A. M. Ivashko* Kak postroit' zashchishchennuyu informatsionnuyu sistemu. – SPb.: Mir i sem'ya – 95, 1997.
 26. Metodicheskie rekomendatsii po vnedreniyu sistemy upravleniya informatsionnoy bezopasnost'yu i metodiki otsenki riskov v sootvetstviy so standartami Natsional'nogo banka Ukrainy: pis'mo departamenta informatizatsii Natsional'nogo banka Ukrainy bankam Ukrainy ot 3 marta 2011 № 24–112/365. – M.: Natsional'nyy bank Ukrainy, 2011.
 27. *A. V. Potiy, A. V. Lenshin* Issledovanie metodov otsenki riskov bezopasnosti informatsii i razrabotka predlozheniy po ikh sovershenstvovaniyu na osnove sistemnogo podkhoda//Sbornik nauchnykh trudov KhUVS, Ed. 2 (24), p. 85–91, 2010.
 28. ISO/IEC 27005 – Information technology – Security techniques – Information security risk management. URL: <http://www.bank.gov.ua/doccatalog/document?id=72235https://exebit.files.wordpress.com/2013/11/iso-27005-2011-ru-v1.pdf>. Accessed on: 09.12.2017.
 29. Rukovodyashchiy dokument. Bezopasnost' informatsionnykh tekhnologiy. Kriterii otsenki bezopasnosti informatsionnykh tekhnologiy. GOST R ISO/MEK 15408–2–2008. URL: <http://primorsky.ru/authorities/executive-agencies/departments/information-security/Documents/doki-po-ib/>. Accessed on: 7.12.2017.
 30. *M. Kobzar', A. Sidak* Metodologiya otsenki bezopasnosti informatsionnykh tekhnologiy po obshchim kriteriyam//Informatsionnyy byuleten' Jet Info, Ed. 6 (133), p. 2–16, 2004.
 31. Rukovodyashchiy dokument. Bezopasnost' informatsionnykh tekhnologiy. Obshchaya metodologiya otsenki bezopasnosti informatsionnykh tekhnologiy. Proekt. URL: <http://fstec.ru/component/attachments/download/293>. Accessed on: 7.12.2017.

32. RS BR IBBS-2.2–2009. Metodika otsenki riskov narusheniya informatsionnoy bezopasnosti. URL: http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf. Accessed on: 7.12.2017.
33. Standart Ukrainy SOU N NBU 65.1 SUIB 1.0: 2010. Metody zashchity v bankovskoy deyatelnosti sistema upravleniya informatsionnoy bezopasnost'yu. Trebovaniya. (ISO/IEC 27001:2005, MOD). – K.: NBU, 2010.
34. Postanovlenie Pravitelstva Natsional'nogo banka Ukrainy ot 18 iyunya 2003 goda № 254 "Ob utverzhdenii Polozheniya ob organizatsii operatsionnoy deyatelnosti v bankakh Ukrainy". – K.: NBU, 2003.
35. The doctrine of information security of Ukraine, approved by the Decree of the President of Ukraine dated February 25, 2017, No. 47/2017. URL: <http://zakon3.rada.gov.ua/laws/show/47/2017/paran2#n2>. Accessed on: 7.12.2017.
36. Ukaz Prezidenta Ukrainy ot 15 marta 2016 № 96 "O reshenii Soveta natsional'noy bezopasnosti i oborony Ukrainy ot 27 yanvarya 2016 goda «O Strategii kiberbezopasnosti Ukrainy»". URL: <http://zakon3.rada.gov.ua/laws/show/96/2016/paran11#n11>. Accessed on: 7.12.2017.
37. Decree of the President of Ukraine dated February 12, 2007 No. 105 "On the Strategy of National Security of Ukraine". URL: <http://zakon3.rada.gov.ua/laws/show/105/2007>. Accessed on: 7.12.2017.
38. R. V. Grishchuk, Yu. G. Danik Sinergiya informatsionnykh i kiberneticheskikh deystviy//Proceedings of the NUOU, № 6 (127), p. 132–143, 2014.
39. V. L. Buryachok, R. V. Grishchuk, and V. A. Khoroshko Politika informatsionnoy bezopasnosti/edited by prof. V. A. Khoroshko. – K.: ChPP «Zadruga», 2014.
40. Yu. G. Danik and others Osnovy zashchity informatsii. Schoolbook. – Zhitomir: ZhVI DUT, 2015.
41. A. K. Yudin Informatsionnaya bezopasnost'. Normativno-pravovoe obespechenie. – M.: NAU, 2011.
42. I. S. Ivanchenko, V. A. Khoroshko, Yu. E. Khokhlachova, D. V. Chirkov Obespechenie informatsionnoy bezopasnosti gosudarstva/edited by prof. V. A. Khoroshko – K.: ChPP "Zadruga" 2013.
43. A. G. Korchenko, A. E. Arkhipov, Yu. A. Dreys Otsenivanie vreda natsional'noy bezopasnosti Ukrainy v sluchae utehki gosudarstvennoy tayny. Monografiya. – K.: NA SBU Ukrainy, 2014.
44. A. A. Korchenko, L. N. Skachek, V. A. Khoroshko Bankovskaya bezopasnost. Uchebnik/edited by prof. V. A. Khoroshko. – K.: ChPP "Zadruga", 2014.
45. V. I. Yarochkin Bezopasnost' bankovskikh sistem. – M.: Publisher: Os'-89, 416 p., 2012.

46. S. Evseev Metodologiya otsenivaniya bezopasnosti informatsionnykh tekhnologiy avtomatizirovannykh bankovskikh sistem Ukrainy// Nauchno-tekhnicheskii zhurnal "Zashchita informatsii", vol. 22, № 2, p. 297–309, 2016.
47. S. Evseev Model' narushitelya prav dostupa v avtomatizirovannoy bankovskoy sisteme na osnove sinergeticheskogo podkhoda//Informatsionnaya bezopasnost', № 2(26), p. 110–120, 2017.
48. S. Evseev Sinergeticheskaya model' otsenki bezopasnosti bankovskoy informatsii//Informatsionnaya bezopasnost', № 4(24), p. 104–118, 2016.
49. Bank dannykh ugroz bezopasnosti informatsii. URL: <http://bdu.fstec.ru/vul>. Accessed on: 5.12.2017
50. R. Grishchuk, S. Evseev Metodologiya postroeniya sistemy obespecheniya informatsionnoy bezopasnosti bankovskoy informatsii v avtomatizirovannykh bankovskikh sistemakh//Bezopasnost' informatsii, 2017.
51. A. K. Yudin, S. S. Buchik, A. V. Chunarev, A. I. Varchenko Metodologiya postroeniya klassifikatora ugroz gosudarstvennym informatsionnym resursam//Naukoemkie tekhnologii, № 2(22), p. 200–210, 2014.
52. A. K. Yudin, S. S. Buchik Klassifikatsiya ugroz gosudarstvennym informatsionnym resursam normativno-pravovogo napravleniya. Metodologiya postroeniya klassifikatora//Zashchita informatsii, Vol. 17(2), p. 108–116, 2015.
53. S. S. Buchik Teoreticheskie osnovy analiza riskov dereva identifikatorov gosudarstvennykh informatsionnykh resursov//Naukoemkie tekhnologii, № 1(29), p. 70–77, 2016.
54. S. S. Buchik Metodologiya analiza riskov dereva identifikatorov gosudarstvennykh informatsionnykh resursov//Zashchita informatsii, № 1(18), p. 81–89, 2016.
55. S. S. Buchik Metodika ekspertnogo otsinyuvannya funktsional'nykh profiliv zagroz derzhavnikh informatsiynykh resursiv//Otkrytye informatsionnye i komp'yuternye integrirovannye tekhnologii, № 70, p. 271–280, 2015.
56. G. V. Grishchuk Teoreticheskie osnovy modelirovaniya protsessov napadeniya na informatsiyu metodami teorii differentsial'nykh igr i differentsial'nykh preobrazovaniy. – Zhitomir: Ruta, 2010.
57. O. Petrov, V. Lakhno Povyshenie informatsionnoy bezopasnosti avtomatizirovannykh sitsem obrabotki dannykh na transporte//Information Technology in Selected Areas of Management. – Krakow: Wydawnictwa AGH, p. 65–78, 2016.
58. G. M. Khmelevskiy Issledovanie otsenki ugroz informatsionnoy bezopasnosti ob'ektov informatsionnoy deyatel'nosti//Zashchita informatsii, № 4, p. 65–70, 2016.

59. V. G. Zhukov, M. N. Zhukova, V. V. Zolotarev, and I. V. Kovalev, Methods of constructing a security model of automated systems, Software products and systems, No. 2, p. 70–74, 2012.
60. V. G. Zhukov, M. N. Zhukova, A. P. Stefarov Model' narushitelya prav dostupa v avtomatizirovannoy sisteme//Programmnye produkty i sistemy, № 2, p. 75–78, 2012.
61. M. N. Zhukova, N. A. Koromyslov Model' otsenki zashchishchennosti avtomatizirovannoy sistemy s primeneniem apparata nechetkoy logiki//Izvestiya YuFU. Tekhnicheskie nauki, № 12 (149), p. 63–69, 2013.
62. S. Mel'nik Kontseptual'nye osnovy organizatsii kriptograficheskoy zashchity informatsii//Nauchnye zapiski Ukrainskogo nauchno-issledovatel'skogo instituta svyazi, № 6, p. 19–26, 2015.
63. A. Potiy Etalonnaya model' sistemy protsessov zashchity informatsii//Pravovoe, normativnoe i metrologicheskoe obespechenie sistemy zashchity informatsii v Ukraine: nauchno-tekhnichestkiy sbornik, Ed. 1 (12), p. 17–30, 2006.
64. A. Potiy, A. Lenshin Metodika otsenki sootvetstviya tekushchey zrelosti tselevym orientiram//Pravovoe, normativnoe i metrologicheskoe obespechenie sistemy zashchity informatsii v Ukraine: nauchno-tekhnichestkiy sbornik, Ed. 1 (12), p. 31–43, 2006.
65. A. V. Daurtsev Razrabotka matematicheskikh modeley otsenki pokazateley effektivnosti programmnykh sistem zashchity informatsii v avtomatizirovannykh sistemakh elektronnoho dokumentooborota. URL: <http://cyberleninka.ru/article/n/razrabotka-matematicheskikh-modeley-otsenki-pokazateley-effektivnosti-programmnyh-sistem-zashchity-informatsii-v-avtomatizirovannykh>. Accessed on: 5.12.2017.
66. V. V. Karpov Veroyatnostnaya model' otsenki zashchishchennosti sredstv vychislitel'noy tekhniki s apparatno-programmnym kompleksom zashchity informatsii ot nesanktsionirovannogo dostupa//Programmnye produkty i sistemy, № 1, p. 31–36, 2003.
67. P. N. Devyanin Modeli bezopasnosti komp'yuternykh sistem. Schoolbook. – M.: Publ. center «Akademiya», 2005.
68. N. A. Gaydamakin Teoreticheskie osnovy komp'yuternoy bezopasnosti. – Ekaterinburg: Publ. center Ural. Un-ta, 2008.
69. P. V. Revenkov Zashchita informatsii v banke: osnovnye ugrozy i bor'ba s nimi. URL: <http://www.crmdaily.ru/novosti-rynka-crm/568-zashchita-informacii-v-banke-osnovnye-ugrozy-i-borba-s-nimi.html>. Accessed on: 5. 12.2017.
70. V. S. Atkina Model' zashchishchennosti organizatsiy bankovskoy sistemy Rossiyskoy Federatsii//Izvestiya YuFU. Tekhnicheskie nauki, Ed. 12 (149), p. 187–193, 2013.

71. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375. Accessed on: 09.12.2017.
72. *R. A. Nurdinov, T. N. Batova* Podkhody i metody obosnovaniya tselesoobraznosti vybora sredstv zashchity informatsii//Sovremennye problemy nauki i obrazovaniya. URL: <http://elibrary.ru/item.asp?id=21285749>. Accessed on: 7.12.2017.
73. RS BS IBBS – 2.2–2009. Obespechenie informatsionnoy bezopasnosti organizatsiy bankovskoy sistemy Rossiyskoy Federatsii. Metodika otsenki riskov narusheniya informatsionnoy bezopasnosti. URL: www.cbr.ru/credit/gubzi_docs/st22_09.pdf. Accessed on: 7.12.2017.
74. *Yu. F. Katorin, R. A. Nurdinov, N. M. Zaytseva* Model' kolichestvennoy otsenki riskov bezopasnosti informatsionnoy sistemy. URL: <http://www.vestnikmnk/index.php/VMK/article/download/57/56>. Accessed on: 7.12.2017.
75. ISO/IEC 18045:2014 Information technology – Security techniques – Guidelines for cybersecurity. URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46412. Accessed on: 09.12.2017.

CHAPTER 3. Development approaches to security banking services in automated banking system on hybrid crypto-code designs from unprofitable codes

3.1 Setting properties crypto-code systems geometrical codes

The main advantage of symmetrical and asymmetrical theoretical coding schemes (TCS) is a high-speed data conversion and maintenance of integrated probability and information secrecy (confidentiality) that meets the basic requirements of IS SI in ABS. General classification methods crypto conversions IP shown in Fig. 3.1.

To ensure information security SI in ABS promising area is the use of asymmetric cryptosystems based TCS McEliece and Niederreiter providing integrated (a mechanism) indicators of reliability at 2^9 – 2^{12} and reliability — 2^{30} – 2^{35} group operations during its construction over the field $GF(2^{10})$. Fig. 3.2 These results cryptoconversions modern performance symmetric and asymmetric cryptosystems. Table 3.1 shows the results of comparative studies of the effectiveness of cryptographic methods of information security at a fixed level stability:

- average (best known difficulty of cryptanalysis algorithms at least 2^{128} operations);
- high (difficulty of cryptanalysis best known algorithm at least 2^{256} operations);
- ultra-high (difficulty of cryptanalysis best known algorithm at least 2^{512} operations).

Table 3.1. — The results of comparative studies of the effectiveness of cryptographic methods of information security at a fixed level stability

Methods crypto-graphic transformation	Security model	The length of the key data bits	Speed of the cryptopereet-vorene., bit/s	Additional features
Block ciphers, symmetric	Practical safety	128, 256, 512	10^6 – 10^9	Do not have
Stream ciphers, symmetric	Practical safety	128, 256, 512	10^7 – 10^{10}	Do not have
Asymmetric RSA-like crypto algorithms	Evidence-Based security	3248 (128), 15424 (256)	10^2 – 10^3	Do not have
Asymmetric CCR using code constructions	Evidence-Based security	$0.5 \cdot 10^6$ (128), $2 \cdot 10^6$ (256)	10^6 – 10^8	Control errors, increasing reliability

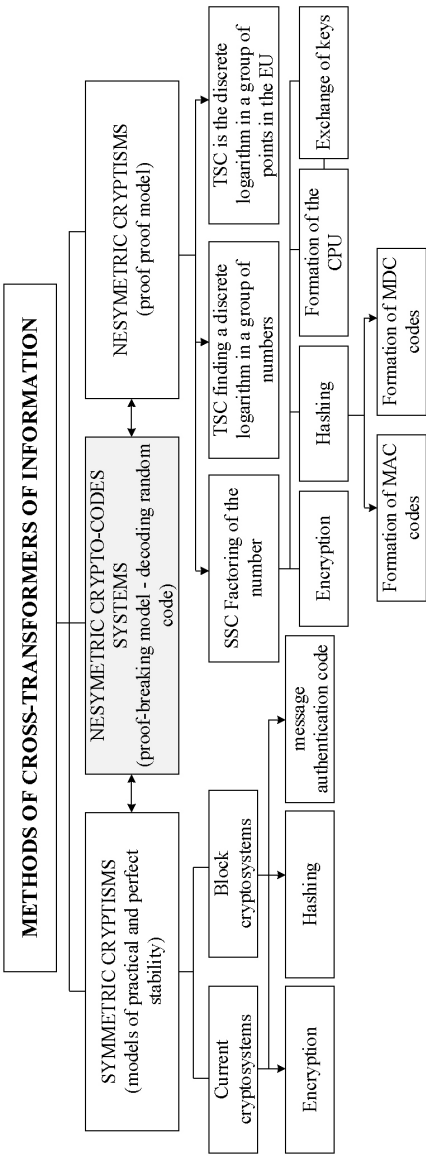


Fig. 3.1. General classification methods cryptoconversion IP



Fig. 3.2. The analysis of speed data conversion

Thus, as follows from the results of comparative analysis (Fig. 3.2 and Table 3.1) asymmetric crypto algorithms using TCR can realize data encryption public key technology and provide the speed crypto-code conversion information with speed encryption BSC. In addition, practical use NCCS information security allows integration mechanisms based on channel coding and encryption comprehensively ensure the safety and reliability of the data.

Consider the overall design of theoretical coding schemes (TCS). Fix a finite field $GF(q)$. Consider the vector space $GF^n(q)$ a plurality of n -sequence elements from $GF(q)$ of the component — wise addition and multiplication by a scalar. Linear (n, k, d) code C is a subspace in $GF^n(q)$, is non-empty set of n -sequences (code words) over $GF(q)$, k — dimension linear subspace, d — minimum code length (the minimum weight of the non-zero coded word).

Linear subspace. That identifies the code C is orthogonal complement, basis of which is set by checking the code matrix H C is a matrix of rank $\text{rank}(H) = r$, $r = n - k$. The dimension checking matrix $r \times n$, and $G \times H^T = 0$. If we consider the matrix H as a set of basis vectors of a linear subspace, we obtain a linear code $C^\perp$ called dual north arbitrary sequence of $n - C$ is a code word C code then, if each line checking orthogonal matrix H is $c \times H^T = 0$. The vector S , called a syndrome coding theory, can be calculated by multiplying the codeword with error $c^* = c + e$ to test the transposed matrix H code: $S = c^* \times H^T = c \times H^T + e \times H^T = e \times H^T$, where e — vector errors, c^* — distorted codeword errors.

Obviously, the value of the syndrome depends on the error vector and is independent of the codeword.

Geometrical codes have good asymptotic properties. With increasing power of the alphabet code symbols asymptotic properties of these codes are improved. Obviously, the great length of these codes are above the Varshamova Gilbert, indicating a high potential characteristics of these codes. Thus, encoding geometrical codes enhances reliability SI in ABS is one of the promising areas. The largest energy effects of coding noise immunity is achieved when using large length codes [1, 2, 34, 35, 36, 37, 38]. Geometrical length code sets the number of points of projective curve, based on which the code [4, 16, 24, 30].

Let $X(GF(q))$ — set point curve X over a finite field $GF(q)$, $N = |X(GF(q))|$ — their number. Number N points of the curve X over $GF(q)$ restricted expression top [41, 42, 43]:

$$N \leq 2\sqrt{q} \cdot g + q + 1, \quad (3.1)$$

where g — generation curve.

Fix a finite field $GF(q)$. Let X — smooth projective algebraic curve in the project area P^n i.e a set of solutions $p_1(x_0, x_1, \dots, x_n)$, $p_2(x_0, x_1, \dots, x_n) \dots$,

$p_N(x_0, x_1, \dots, x_n), \forall p \in P^n$ irreducible homogeneous system of algebraic equations with coefficients $\deg X$ degree of $GF(q)$.

Table. 3.3 shows the kind of upper bound g curve X .

Table 3.3. — Upper kind of evaluation g curve X in P^n

$\deg X$	$g(P^2)$	$g(P^3)$	$g(P^4)$	$g(P^5)$	$g(P^6)$
2	0	—	—	—	—
3	1	0	—	—	—
4	3	1	0	—	—
5	6	2	1	0	—
6	10	4	2	1	0
7	15	6	3	2	1
8	21	9	5	3	2
9	28	12	7	4	3
10	36	16	9	6	4

Table 3.4 shows the upper estimate of the number of points of the curve over a finite field.

Table 3.4. — Evaluation upper limit of the number of points a smooth projective curve

g	$\deg X$	$N = X(GF(q)) $				
		$GF(4)$	$GF(8)$	$GF(16)$	$GF(32)$	$GF(64)$
0	2	5	9	17	33	65
1	3	9	14	25	44	81
2	4	10	18	33	53	97
3	4	17	24	41	66	113
4	5	21	29	49	77	129
5	5		34	57	88	145
6	5		39	65	99	164
7	6		44	73	110	180
8	6		49	81	121	196
9	6		54	89	132	212
10	6		59	97	143	228
11	7		64	105	154	244
12	7		69	113	165	260
13	7			121	176	276
14	7			129	187	292
15	7			137	198	308

The general scheme of coding geometrical first proposed in [45]. Let C — Class on dyvivoriv X degree α . Then C sets display $\phi: X \rightarrow P^m$ Set function generator $y_i = \phi(x_i)$ length code sets geometrical $n \leq N$. Coded characteristics (n, k, d) are related $k + d \geq n - g + 1$. If $2g - 2 < \alpha \leq n$ Code related characteristics $(n, \alpha - g + 1, d), d \geq n - \alpha$.

We give the following definition geometrical code.

Property 1 [1, 2]. Let X — smooth projective algebraic curve in the project space P^n , is the set of solutions of a homogeneous irreducible algebraic equation $\deg X$ degree with coefficients in $GF(q)$. Consider the variety corresponding projective hypersurface, given P^n in the equation $F=0$, where F — homogeneous monomials degree $\deg F$. Let $I(i_1, i_2, \dots, i_n)$ — sequence information. Geometrical code curve X over $GF(q)$ — linear code of length $n \leq N$, code words $C(c_1, c_2, \dots, c_n)$ is defined by equality:

$$\sum_{i=0}^{k-1} i_j F_j(P_i) = c_i, \quad (3.2)$$

where $P_i(X_i, Y_i, Z_i)$ — projective curve point X , which is (X_i, Y_i, Z_i) — a homogeneous solution of algebraic equations that define the curve X , $i = \overline{1, n}$; $F_j(P_i)$ — value generator functions at the points curve.

This definition is equivalent matrix representation geometrical code [1, 2]:

$$G(i_0, i_1, \dots, i_{k-1})^T = (c_0, c_1, \dots, c_{n-1}), \quad (3.3)$$

where G — generative matrix of dimension $k \times n$, $K = \alpha - g + 1$, $\alpha = \deg X \cdot \deg F$ species:

$$G = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{k-1}(P_0) & F_{k-1}(P_1) & \dots & F_{k-1}(P_{n-1}) \end{pmatrix} = \|F_j(P_i)\|_{n,k}. \quad (3.4)$$

Property 2 [1, 2]. Elliptic curve (EC) in affine space A^2 over the field $GF(q)$ is called a smooth curve defined by the equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (3.5)$$

or P^2 defined homogeneous equation:

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3, \quad (3.6)$$

$a_i \in GF(q)$, the genus of the curve $g = 1$.

Statement 1 [1, 2]. Geometrical (n, k, d) code elliptic curve (elliptic code) over $GF(q)$ built through the display view $\varphi: EC \rightarrow P^{k-1}$ related characteristics $k + d \geq n$, And: $n \leq 2\sqrt{q} + q + 1$, $k \geq \alpha$, $d \geq n - \alpha$, $\alpha = 3 \cdot \deg F$.

Proof. Let EC — smooth projective elliptic curve in the project area P^2 over $GF(q)$, $g = g(EC) = 1$, $EC(GF(q))$ — the set of points over $GF(q)$, $N = EC(GF(q))$ — their number. By Theorem Khase Vale number of points a smooth projective curve of genus g in P^2 over $GF(q)$ is bounded above expression $N \leq 2g\sqrt{q} + q + 1$. For elliptic curve will look like this expression $N \leq 2\sqrt{q} + q + 1$. By definition, $n \leq N$ respectively $n \leq 2\sqrt{q} + q + 1$.

Let C — Class degree in EC $\alpha > 0$. Then C determines display $\varphi: X \rightarrow P^{k-1}$ where $k \geq \alpha$. Sets $y_i = \varphi(X_i)$ sets the code. The number of points in the intersection $\varphi(EC)$ with equal hyperplane α , i.e. $n - d \leq \alpha$. Thus, parameters geometrical code for elliptic curve are related by $k + d \geq n$, And $d \geq n - \alpha$. Degree $\deg EC = 3$, respectively, $\alpha = 3 \cdot \deg F$.

Property 3 [1, 2]. Let X — smooth projective algebraic curve in P_n , i.e. the set of solutions of a homogeneous irreducible algebraic equation of degree $\deg X$ with coefficients from $GF(q)$, F — homogeneous monomials degree $\deg F$. Geometrical code curve X over $GF(q)$ — a linear code, consisting of all words $(C_1, C_2, \dots, C_N)$ of length $n \leq N$, for which the equality $d + g - 1$ equations:

$$\sum_{i=0}^{n-1} c_i F_j(P_i) = 0, \quad (3.7)$$

where $SI \in GF(q)$, $d \geq \alpha - 2g + 2$, $\alpha = \deg X \cdot \deg F$.

This definition is equivalent matrix presentation geometrical code:

$$H(c_0, c_1, \dots, c_{n-1})^T = 0, \quad (3.8)$$

where H — the verification code matrix dimension $r \times n$, $R = n - k = d + g - 2$:

$$H = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{r-1}(P_0) & F_{r-1}(P_1) & \dots & F_{r-1}(P_{n-1}) \end{pmatrix} = \|F_j(P_i)\|_{n,r}. \quad (3.9)$$

Statement 2. [1, 2]. Elliptical (n, k, d) code over $GF(q)$, built through the reflection type $\varphi: EC \rightarrow Pr - 1$ related characteristics $k + d \geq n$, And: $n \leq 2\sqrt{q} + q + 1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \cdot \deg F$.

Structural characteristics of elliptical codes constructed through the display view $\varphi: EC \rightarrow P^{k-1}$ over $GF(q)$, $q = 2^m$, $m = \overline{2, 6}$ are shown in Table. 3.5. Output of construction geometrical codes (AHA) (modified AHA) are presented in the Addition B.

The main purpose of encoding information is control (detection and correction) of errors that occurred during the message transmission on the channel

noise. For error checking Encoder introduces redundancy (Verification of length $r, r = n - k$) in the transmitted data. On the receiving side, analyzing the properties and checking of their compliance data transmitted, decoder reduces the impact of errors encountered during transmission.

Table 3.5. — Design characteristics Combination elliptical codes constructed through reflection $\varphi: EC \rightarrow P^{k-1}$ over $GF(q), q = 2^m, m = \overline{2, 6}$

<i>degF</i>	α	(n, k, d)				
		<i>GF</i> (4)	<i>GF</i> (8)	<i>GF</i> (16)	<i>GF</i> (32)	<i>GF</i> (64)
1	3	9, 3, 6	14, 3, 11	25, 3, 22	44, 3, 41	81, 3, 78
2	6	9, 6, 3	14, 6, 8	25, 6, 19	44, 6, 38	81, 6, 75
3	9	—	14, 9, 5	25, 9, 16	44, 9, 35	81, 9, 72
4	12	—	14, 12, 2	25, 12, 13	44, 12, 32	81, 12, 69
5	15	—	—	25, 15, 10	44, 15, 29	81, 15, 66
6	18	—	—	25, 18, 7	44, 18, 26	81, 18, 63
7	21	—	—	25, 21, 4	44, 21, 23	81, 21, 60
8	24	—	—	—	44, 24, 20	81, 24, 57
9	27	—	—	—	44, 27, 17	81, 27, 54
10	30	—	—	—	44, 30, 14	81, 30, 51
11	33	—	—	—	44, 33, 11	81, 33, 48
12	36	—	—	—	44, 36, 8	81, 36, 45
13	39	—	—	—	44, 39, 5	81, 39, 42
14	42	—	—	—	44, 42, 2	81, 42, 39
15	45	—	—	—	—	81, 45, 36
16	48	—	—	—	—	81, 48, 33
17	51	—	—	—	—	81, 51, 30
18	54	—	—	—	—	81, 54, 27
19	57	—	—	—	—	81, 57, 24
20	60	—	—	—	—	81, 60, 21
21	63	—	—	—	—	81, 63, 18
22	66	—	—	—	—	81, 66, 15
23	69	—	—	—	—	81, 69, 12
24	72	—	—	—	—	81, 72, 9
25	75	—	—	—	—	81, 75, 6
26	78	—	—	—	—	81, 78, 3

The task of decoding can be effectively resolved (with polynomial complexity) to a narrow class of codes, such as noise codes Bouza-Chowdhury, Hokvynhema (BCH) and Reed-Solomon codes. One of the most efficient algorithms for

decoding algebraic codes are BCH algorithm Berlekempa-Messi and his modification (improvement). It is known [1, 2, 34, 35, 36, 37, 38] Algorithm Berlekempa-Messi implementation contains a number of multiplications, order t^2 , or, formally, algorithm complexity $O(t^2)$, where t — correcting ability of the code, $t = \lfloor (d-1)/2 \rfloor$. For a large accelerated algorithm using t — Berlekempa Messi that reduces the computational complexity of the algorithm. Even more effective in terms of computational complexity, there is a recursive algorithm Berlekempa-Messi. Asymptotic complexity of decoding Reed-Solomon codes in this case does not exceed $O(n \log^2 n)$, and very close to the value of $O(n \log n)$.

Decoding arbitrary linear code (code general provisions) is rather complicated computational problem, the complexity of its solution increases exponentially. Thus, for the correlation decoding arbitrary (n, k, d) code over $GF(q)$ should, in general, compare all the accepted sequence q^k code word and choose the closest (in metric Hemet). Even for small n, k, d and q correlation decoding task is very time consuming. This position is the basis of all cryptographic systems on algebraic block codes. Masking code with fast decoding algorithm (polynomial complexity) at random (random) linear code decoding task imaginable for an outside observer (possible attacker) in computing challenger (exponential complexity).

3.1.1 Setting properties asymmetric crypto code of McEliece and Niederreiter Elliptic codes

Consider a theoretical diagram code (TCS) McEliece, first proposed in [32]. Let G — generative matrix of linear (n, k, d) code over $GF(q)$ with polynomial complexity decoding X — nondegenerate $k \times k$ -matrix over $GF(q)$, D — diagonal matrix with nonzero on the diagonal elements, P — Adjustable matrix of size $n \times n$. Rearrangement matrix implements a permutation vector coordinates as matrix multiplication, namely, the element p_{ij} matrix P is equal to 1 if and only if coordinate with the number i moves using coordinate changes in the number of j . In other cases, $p_{ij} = 0$. Therefore, the matrix P includes in each column and each row only one unit. The product matrix $\Lambda = P \cdot D$ asks permutation matrix Λ with nonzero elements of the field $GF(q)$. Rearrangement matrix Λ (Unipotential 2 matrix) with the permutation vector coordinates keeps distance in Hemet, that $d(a, b) = d(a \cdot \Lambda, b \cdot \Lambda)$. Where $d(x, y)$ — distance in Hemet between vectors x and y .

Public key in asymmetric crypto-code system (NCCS) based TCS McEliece is a generative matrix $Gh = X \times G \times P \times D$, obtained by multiplying generative matrix of linear (n, k, d) code over $GF(q)$ to masking matrix (X, P, D) , personal (private) key is the matrix X, P, D . Classified information is a vector of length n and is calculated according to the rule:

$$c_x^* = i \times G_x + e, \quad (3.10)$$

where: the vector $C_x = i \times G_x$ belonging $Gh(n, k, d)$ code of generative matrix G_x ;

i — k -bit information vector;

the vector e — secret weight vector errors $\leq t$ (secret session key).

Properties 1, 2 and the result first statement allow you to specify NCCS McEliece codes based on elliptic follows [2, 12, 24]. Let GEC — generative elliptic matrix (n, k, d) code over $GF(q)$ of the form:

$$G^{EC} = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{k-1}(P_0) & F_{k-1}(P_1) & \dots & F_{k-1}(P_{n-1}) \end{pmatrix} = \|F_j(P_i)\|_{n,k}, \quad (3.11)$$

and dimension $k \times n$, $k = \alpha$, $\alpha = 3 \cdot \deg F$.

Let X — nondegenerate $k \times k$ matrix over $GF(q)$, D — diagonal matrix with nonzero elements on the diagonal, P — permutation matrix of dimension $n \times n$. Identify NCCS McEliece from the EU, the public key — the matrix $G_x^{EC} = X \times G^{EC} \times P \times D$, Private (secret) key — matrix X, P, D .

Parking information is a vector of length n and is defined by the rule:

$$c_x^* = i \times G_x^{EC} + e,$$

where vector $c_x = i \times G_x^{EC}$, which belongs elliptic (n, k, d) code of generative matrix G_x^{EC} , i — k -bit information vector, the vector e — secret weight vector errors $\leq t$.

Consider a theoretical coding scheme Niederreiter first proposed in [33]. Let H — test matrix of linear (n, k, d) code over $GF(q)$ with polynomial complexity decoding. Let X — nondegenerate $r \times r$ matrix over $GF(q)$, D — diagonal matrix with nonzero elements on the diagonal, P — permutation matrix of size $n \times n$. Open (public) key in TCS Niederreiter the matrix $H_x = X \times N \times P \times D$, personal (private) key matrix is masking — X, P, D . classified information S_x is a syndrome — a vector of length $r = n - k$, which is calculated according to the rule:

$$S_x = e \times H_x^T, \quad (3.12)$$

where vector e — vector of length n and weight $\leq t$, that is confidential information.

Authorized recipient of confidential information (which has its own key) is one of the solutions qk expression $S_x = c_x^* \times H_x^T$. Found decision — code word errors $c_x^* = i \times G_x + e$. Further, as in the diagram McEliece authorized user builds a vector $\bar{c}^* = c_x^* \times D^{-1} \cdot P^{-1}$ and decode received word. However, instead

of restoring the information word i' , it calculates code word $c' = i' \cdot G$ and then the error vector $e' = \bar{c}^* - c'$. The last step is carried calculating the vector $e = e' \times P \times D$, which is confidential.

To set NCCS Niederreiter to use the property EC 3 geometrical representation of code or matrix code are geometrical:

$$H(c_0, c_1, \dots, c_{n-1})^T = 0, \quad (3.13)$$

where H — the verification code matrix dimension $r \times n$, $R = n - k = d + g - 2$:

$$H = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{r-1}(P_0) & F_{r-1}(P_1) & \dots & F_{r-1}(P_{n-1}) \end{pmatrix} = \|F_j(P_i)\|_{n,r}. \quad (3.14)$$

Property 3 and Proposition 2 result (3.4) (3.5) can determine NCCS Niederreiter based on elliptic codes follows.

Let NEC — elliptical test matrix (n, k, d) code over $GF(q)$ of the form (3.14) and dimension $r \times n$, $R = \alpha$, $\alpha = 3 \cdot \deg F$. Let X — nondegenerate $k \times k$ matrix over $GF(q)$, D — diagonal matrix with nonzero elements on the diagonal, P — permutation matrix of size $n \times n$. Define asymmetrically Niederreiter scheme of elliptic code [8]. Public key — matrix - $H_X^{EC} = X \times H^{EC} \times P \times D$, Private (secret) key — matrix X, P, D .

Parking information is a vector of length n and is calculated according to the rule (3.13). To generate the error vector e (confidential information) in [18] the practical algorithms for converting vector information in the error vector on the basis of equilibrium encoding.

Proven assertions 1 and 2 of the proposed EC NCCS allow for asymmetric cryptosystems, public key that is used for the exchange of classified information in the OPS.

General classification crypto-code systems (CCCS) and security services that ensure their use are shown in Fig. 3.3.

However, conducted in [7, 12, 18] analysis software implementation NCCS McEliece and Niederreiter showed considerable complexity of program implementation, which significantly complicates the use of protocols NCCS in ABS.

Research results energy costs (Table 3.6) software implementation, taking into account that the number of processor cycles required to perform 1,000 operations on average, reading — 27 cycles, compared with the — 54 cycles string concatenation — 297 cycles. The calculation is processor clocked at 2 GHz based operating system 5 %.

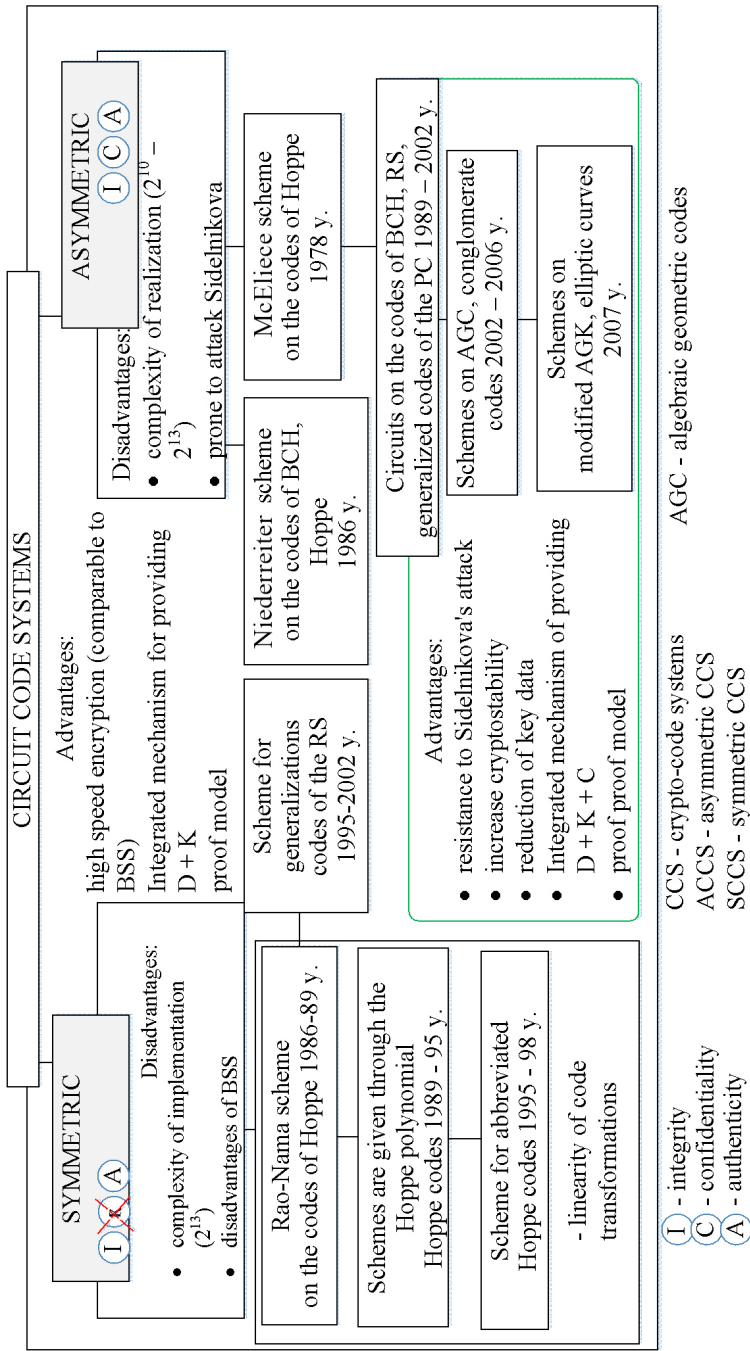


Fig. 3.3. Classification cryptosystems based TCS

Table 3.6. — The evaluation TCS energy costs and McEliece Niederreiter in EU

The length of the code sequence		Niederreiter				McEliece			
Length inform. vector		10	100	1000	10	100	1000	1000	1000
Number of function calls that implement basic operations	Reading symbol	1160342	2502422	11018042	30800328	80859933	159232222		
	Comparison line	381020	777560	3663356	10199898	26364634	4742960		
	Concatenation line	192770	411380	1834983	5125564	13415329	2597480		
Sum		1734132	3691362	23263662	16516381	46125790	120639896		
Length serve in CPU cycles	Reading symbol	31329	67565	297487	831609	2183218	429927		
	Comparison line	20575	41988	197821	550794	1423690	256120		
	Concatenation line	57253	122180	544990	1522293	3984353	771452		
Sum		109157	231733	1457498	1040298	2904696	7591261		
Time for a 10.6 pp		0.06	0.12	0.77	0.55	1.53	4		

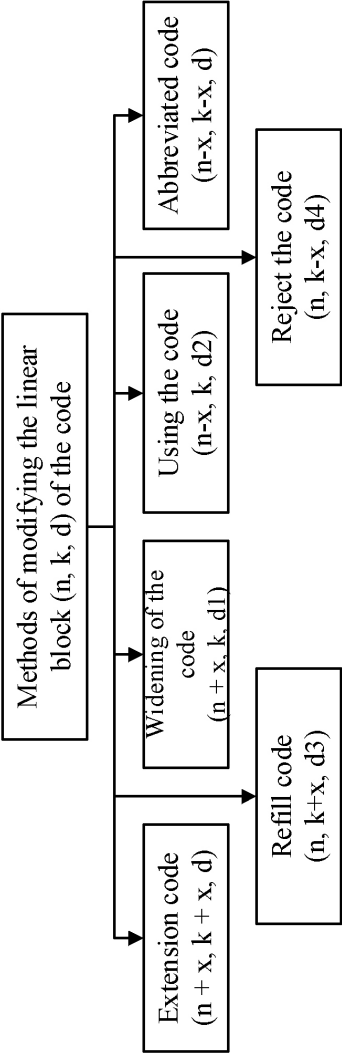


Fig. 3.4. Methods of modifying linear block codes

To collect the submitted values used programming tool for memory debugging, memory leak detection and profiling — Valgrind, namely its module — Callgrind.

To reduce energy consumption in crypto conversions NCCS McEliece in [7] Proposed to use modified NCCS (IAMB) for the modified *EC* (MEC) in the EU.

3.1.2 Development of a method of masking elliptical codes

Known methods modified linear block code more fully discussed in [1, 2, 34, 35, 36, 37, 38]. Fig. 3.4 are the most common ways of modification. Elongation (n, k, d) linear block code is to increase the length $n + x$ by adding new information symbols $k + x$. Expansion (n, k, d) linear block code is to increase the length $n + x$ by adding new check symbols $r + x$.

Deletion (N, k, d) linear block code is to reduce the length $n - x$ by reducing check symbols $r - x$. Reduction of (n, k, d) linear block code is to reduce the length $n - x$ by reducing the information symbols $k - x$. Replenishment (n, k, d) linear block code is to increase the length of the information symbols $k + x$ without increasing the length of the code. Throwing (n, k, d) linear block code is to reduce the information symbols $k - x$ without increasing the length of the code.

Potential resistance is determined by the complexity of decoding NCCS random (n, k, d) block code. Thus, the potential to build sustainable theoretical coding schemes necessary to use methods modifications not allow the reduction of the minimum code distance. Methods of lengthening and shortening of linear block codes do not change the minimum distance, and so allow building resistant to fracture NCCS [1, 2, 7, 12, 15, 30].

We use the definition of elliptic codes [1, 2, 42]. Just following properties:

Property 4. Elliptical (n, k, d) code over $GF(q)$, built through the reflection type $\varphi: EC \rightarrow P^{k-1}$ related characteristics $k + d \geq n$, And: $n \leq 2\sqrt{q} + q + 1$, $k \geq \alpha$, $d \geq n - \alpha$, $\alpha = 3 \cdot \deg F$.

Property 5. Elliptical (n, k, d) code over $GF(q)$, built through the reflection type $\varphi: EC \rightarrow Pr - 1$ related characteristics $k + d \geq n$, And: $n \leq 2\sqrt{q} + q + 1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \cdot \deg F$.

Let A — generating elliptical matrix (n, k, d) code over $GF(q)$ of the form:

$$A = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{M-1}(P_0) & F_{M-1}(P_1) & \dots & F_{M-1}(P_{n-1}) \end{pmatrix} = \|F_j(P_i)\|_{n,M}, \quad (3.15)$$

and dimension $M \times n$, $M = \alpha$, $\alpha = 3 \cdot \deg F$.

To reduce the amount of key data in the theoretical coding scheme on elliptic codes use the following features of the matrix A .

Generating A matrix formed by reflection points of an elliptic curve generating basis functions. Generating an elliptic matrix code, built on a curve:

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3, \quad (3.16)$$

$a_i \in GF(q)$, with polynomial coefficients uniquely define a curve and, accordingly, set design points which built elliptical code (the generator matrix). Fair the following statement.

Statement 3 [7]. Elliptical (n, k, d) code over $GF(q)$ uniquely given set $a_1 \dots a_6, \forall a_i \in GF(q)$.

Bringing. Consider the elliptical generator matrix (n, k, d) code over $GF(q)$:

$$A = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{M-1}(P_0) & F_{M-1}(P_1) & \dots & F_{M-1}(P_{n-1}) \end{pmatrix}. \quad (3.17)$$

Each character generator matrix formed by calculating the value generating function F_j at the point P_i elliptic curve. M number generator functions defined design features elliptical (n, k, d) code. Type of power of the functions F_j determined α display points of the curve and thus the same design parameters given code.

Thus, if the set design (n, k, d) features elliptic code is unique generator matrix defines a set of points $P_1, P_2, \dots, P_n$, which estimated value generating functions. A specific set of points of the space definitely P^2 given type of polynomial curve coefficients is set $a_1 \dots a_6, \forall a_i \in GF(q)$.

Outcome 1. The amount of the private key (in bits) in motivated crypto-code system based on TCS McEliece, based on elliptic (n, k, d) codes over $GF(2^m)$ is the sum of matrix elements X, P, D (in bits) and given by expression:

$$l_{K+} = 5 \times n^2 \times k^2 \times m. \quad (3.18)$$

Bringing. Indeed, the secret key in the scheme of McEliece — generating matrix A (generative matrix) and matrix masking X, P, D . To determine the secret key (in bits) Elliptical (n, k, d) code over $GF(2^m)$, according to 3, enough to define a set of coefficients $a_1 \dots a_6, \forall a_i \in GF(2^m)$ and masking matrix elements. Total should be kept $l_{K+} = 5 \times n^2 \times k^2 \times m$ bits of secret key information.

Expression (3.18) to evaluate the amount of secret key data NCCS McEliece in the EC .

Thus, a method of masking based on building NCCS modified to EC (MNCCS to the EC), which as sensitive data using elliptic curve parameters, can significantly reduce the amount of key data compared with the classical scheme McEliece.

3.1.3 Develop methods modified elliptical codes

The most simple and convenient way to modify the linear block code that does not reduce 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) block code. We define the subset of information symbols $h, |h| = x, X \leq 1/2k$. Put in information vector I in a subset h zero, ie $I_i = 0, \forall I_i \in h$. On the other positions put the vector information symbols. When encoding information symbols set vector h is not involved (they are zero) and can be discarded and the received code-word is shorter in x code symbols. For modifications (shortening) codes will use the elliptical reduction set point curve. Fair the following statement.

Statement 4. Let the EC — elliptic curve over $GF(q), g = g(EC)$ — the family of the curve, $EC(GF(q))$ — the set of points over a finite field, $N = EC(GF(q))$ — their number. Let X and h — disjoint subsets of points, $X \cup h = EC(GF(q)), |h| = x$.

Then truncated elliptical (n, k, d) code over $GF(q)$, built through the reflection type $\varphi: X \rightarrow P^{k-1}$ related characteristics $k + d \geq n$, and: $n \leq 2\sqrt{q} + q + 1, k \geq \alpha - x, d \geq n - \alpha, \alpha = 3 \cdot \deg F$.

Statement 5. Truncated elliptical (n, k, d) code over $GF(q)$, built through the reflection type $\varphi: X \rightarrow P^{r-1}$ related characteristics $k + d \geq n$, and: $n \leq 2\sqrt{q} + q + 1, k \geq n - \alpha, d \geq \alpha, \alpha = 3 \cdot \deg F$.

Using the result of statements 4, 5 MNCCS ask McEliece on modified elliptical codes (MEC), built through the reflection type $\varphi: X \rightarrow P^{k-1}$ and $\varphi: X \rightarrow P^{r-1}$. Just following statement.

Statement 6. Truncated elliptical (n, k, d) code over $GF(2^m)$, built through the reflection type $\varphi: X \rightarrow P^{k-1}$ determines MNCCS to MEC with parameters: the secret key dimensions:

$$l_{k+} = x \cdot \left\lceil \log_2 \left(2\sqrt{q} + q + 1 \right) \right\rceil; l_i = (\alpha - x) \cdot m. \quad (3.19)$$

Dimension vector information (in bits):

$$l_i = (\alpha - x) \times m. \quad (3.20)$$

Codogram dimension:

$$l_s = \left(2\sqrt{q} + q + 1 - x \right) \cdot m. \quad (3.21)$$

The relative speed of coding:

$$R = (\alpha - x) / \left(2\sqrt{q} + q + 1 - x \right). \quad (3.22)$$

Statement 7. Truncated elliptical (n, k, d) code over $GF(2^m)$, built through the reflection type $\varphi: X \rightarrow P^{r-1}$, built through display type:

Private key dimension is defined by (3.20);

Dimension vector information (in bits):

$$l_i = (2\sqrt{q} + q + 1 - \alpha) \times m; \quad (3.23)$$

Codogram dimension is defined by (3.21);

Relative speed:

$$R = (2\sqrt{q} + q + 1 - \alpha) / (2\sqrt{q} + q + 1 - x). \quad (3.24)$$

Consider formal description MNCCS McEliece through the use of methods and practical modifications formation algorithms to ensure privacy SI in ABS.

Mathematical model NCCS using TCS McEliece-based shortening (reduction information symbols) formally given the totality of these elements [7]:

– the set of open-source — $M = \{M_1, M_2, \dots, M_{q^k}\}$, where

$M_i = \{I_0, I_{h_1}, \dots, I_{h_j}, I_{k-1}\}$, $\forall I_i \in GF(q)$; h_j — information symbols are zero, $|h| = \frac{1}{2}k$, that is $I_i = 0$, $\forall I_i \in h$;

– set closed texts (codogram) — $C = \{C_1, C_2, \dots, C_{q^k}\}$, where

$C_i = (A_{X_0}^*, A_{h_1}^*, \dots, A_{h_j}^*, A_{X_{n-1}}^*)$, $\forall A_{X_j}^* \in GF(q)$;

– set direct mappings (based on the use of public key — generative matrix): $\phi = \{\phi_1, \phi_2, \dots, \phi_s\}$, where $\phi_i : M \rightarrow C_{k-h_j}$, $i = 1, 2, \dots, s$; $i = 1, 2, \dots, s$;

– set of inverse mapping (through the use of closed (private) key — masking matrix): $\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, \dots, \phi_s^{-1}\}$, where $\phi_i^{-1} : C_{k-h_j} \rightarrow M$, $i = 1, 2, \dots, s$;

– a set of keys that parameterize direct reflection (public key authorized user): $K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, \dots, K_{s_{a_i}}\} = \{G_X^{EC_1}, G_X^{EC_2}, \dots, G_X^{EC_s}\}$, where $G_X^{EC_i}$ — generative $n \times k$ Matrix disguised random code block geometrical (n, k, d) with elements of the code $GF(q)$, i.e. $\phi_i : M \xrightarrow{K_{ia_i}} C_{k-h_j}$; $i = 1, 2, \dots, s$; a_i — a set of polynomial curve coefficients $a_1 \dots a_s$, $\forall a_i \in GF(q)$ clearly poses a specific set point curve space P^2 ;

– a set of keys that parameterize reverse mapping (private (secret) key authorized user):

$$K^* = \{K_1^*, K_2^*, \dots, K_s^*\} = \{\{X, P, D\}_1, \{X, P, D\}_2, \dots, \{X, P, D\}_s\},$$

$$\{X, P, D\}_i = \{X^i, P^i, D^i\}, \quad (3.25)$$

where X^i — masking nondegenerate randomly generated equally probable source keys $k \times k$ matrix elements of $GF(q)$; P^i — rearrangement randomly generated equally probable source keys $n \times n$ matrix elements of $GF(q)$;

D^i — diagonal matrix formed from a source key elements of $GF(q)$; that is $\phi_i^{-1} : C \xrightarrow{K_i^*} M$, $i = 1, 2, \dots, s$, the complexity of reverse mapping ϕ_i^{-1} without knowledge of the key $K_i^* \in K^*$ related to the decision-theoretic challenger decoding the random code (code common position).

Initial data considered in describing the asymmetric crypto-code information protection system are:

- geometrical block (n, k, d) code C_{k-h_j} over $GF(q)$, i.e. the set of code words $C_i \in C_{k-h_j}$ such that the equality $C_i H^T = 0$, where H — test matrix geometrical block code;

- a_i — a set of polynomial curve coefficients $a_1 \dots a_6$, $\forall a_i \in GF(q)$ clearly poses a specific set point curve P^2 space to form a matrix that generates;

- h_j — information symbols are zero, $|h| = \frac{1}{2}k$, i.e. $I_i = 0$, $\forall I_i \in h$;

- masking matrix display given set of matrices $\{X, P, D\}_i$, where X — non-degenerate $k \times k$ matrix over $GF(q)$, P — rearrangement $n \times n$ matrix over $GF(q)$ with a non-zero element in each row and each column of the matrix, D — diagonal $n \times n$ matrix over $GF(q)$ with nonzero elements on the main diagonal.

In MNCCS McEliece modified (shortened) geometrical (n, k, d) code C_{k-h_j} with fast decoding algorithm disguised as random (n, k, d) code $C_{k-h_j}^*$ by multiplying generative matrix of code GES C_{k-h_j} for masking matrix that are in secret X^u , P^u and D^u [7] to form the public key of the authorized user:

$G_X^{ECu} = X^u \cdot G^{EC} \cdot P^u \cdot D^u$, $u \in \{1, 2, \dots, s\}$, where G^{EC} — generative $n \times k$ geometrical block matrix (n, k, d) with elements of the code $GF(q)$ built on the basis of user-selected polynomial curve coefficients $a_1 \dots a_6$, $\forall a_i \in GF(q)$ clearly that define a specific set point curve space P^2 .

Forming a closed text $C_j \in C_{k-h_j}$ introduced by the plaintext $M_i \in M$ and given public key G_X^{ECu} , $u \in \{1, 2, \dots, s\}$ carried out by forming a code word masked with adding code to it randomly generated vector $e = (e_0, e_1, \dots, e_{n-1})$:

$C_j = \phi_u(M_i, G_X^u) = M_i \cdot (G_X^u)^T + e$, Hemet and weight (the number of non-zero elements) vector e does not exceed the capacity used algebraic correcting code block: $0 \leq w(e) \leq t = \left\lfloor \frac{d-1}{2} \right\rfloor$, $\lfloor x \rfloor$ — the whole of real numbers x .

For each closed text which formed $C_j \in C_{k-h_j}$ corresponding vector $e = (e_0, e_1, \dots, e_{n-1})$ acts as a one-time session key that is specific to E_j vector e formed by accident, equally probable and closed independently of the other texts.

In the channel coming $C_j^* = C_j - C_{k-h_j}$.

On the receiving side the authorized user who knows masking rule, the number and location information null characters can use speed decoding algorithm geometrical code (polynomial complexity) to recover the plaintext [7]:

$$M_i = \phi_u^{-1}(C_j^*, \{X, P, D\}_u).$$

To restore the plaintext authorized user adds zero information symbols $C_j^* = C_j + C_{k-h_j}$, recovered from a closed text C_j takes action secret permutation and diagonal matrices P^u and D^u :

$$\begin{aligned} C &= C_j^* \cdot (D^u)^{-1} \cdot (P^u)^{-1} = (M_i \cdot (G_X^u)^T + e) \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \\ &= (M_i \cdot (X^u \cdot G \cdot P^u \cdot D^u)^T + e) \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \\ &= M_i \cdot (X^u)^T \cdot (G)^T \cdot (P^u)^T \cdot (D^u)^T \cdot (D^u)^{-1} \cdot (P^u)^{-1} + e \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \\ &= M_i \cdot (X^u)^T \cdot (G)^T + e \cdot (D^u)^{-1} \cdot (P^u)^{-1}. \end{aligned} \quad (3.27)$$

Decode received vector algorithm Berlekempa-Messi [34, 35, 36]:

$$C = M_i \cdot (X^u)^T \cdot (G^{EC})^T + e \cdot (D^u)^{-1} \cdot (P^u)^{-1}. \quad (3.28)$$

That gets rid of the second term and the multiplier $(G)^{EC^T}$ in the first term on the right side of equality, then remove the masking effect of the matrix X^u . For the result of decoding $M_i \cdot (X^u)^T$ be multiplied by $(X^u)^{-1}$: $(M_i \cdot (X^u)^T) \cdot (X^u)^{-1} = M_i$. The resulting solution — are plain text M_i .

Block diagram of protocol information in real time using MNCCS McE-
liece with modified (shorter) elliptical codes shown in Fig.3.5.

Fig. 3.6 The algorithm formation cryptograms/codogram algorithm to de-
code MNCCS McEliece with short MEA shown in Fig. 3.7.

The second way to modify the linear block code that stores the minimum code distance and increases the amount of data transferred is extending its length after forming initialization vector, by reducing the information symbols. Let $I = (I_1, I_2, \dots, I_k)$ — information vector $((n, k, d)$ block code. Let's choose a subset of information symbols $h, |h| = x, X \leq k$ and form the initialization vector.

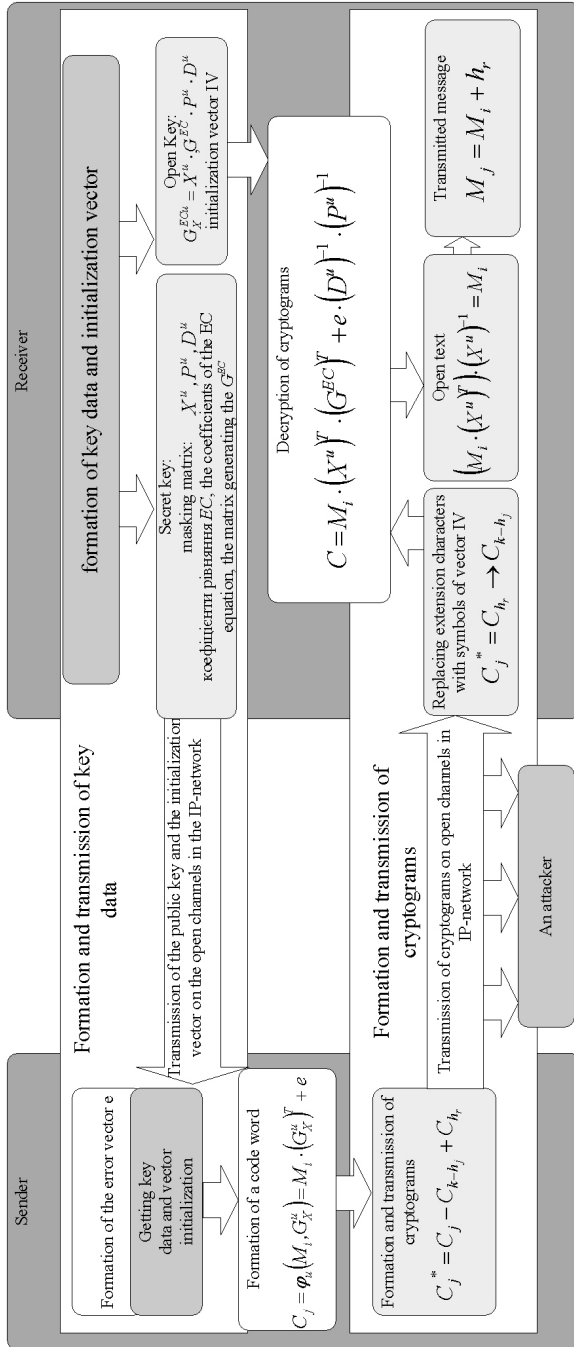
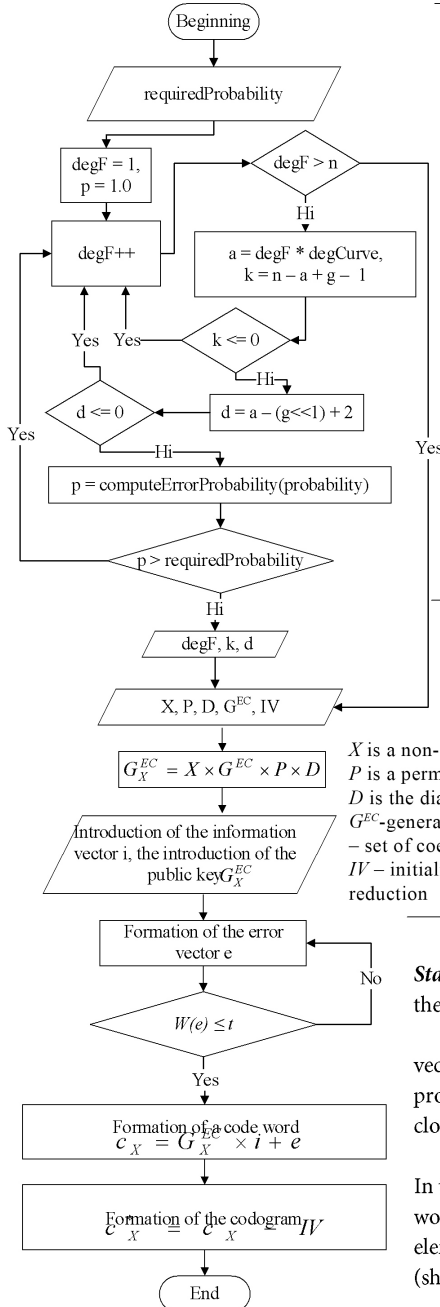


Fig. 3.5. Block diagram of protocol information in real time using MNCCS McEliece with short MEC



Stage 1. Setting the code parameters

Required Probability - The probability of block distortion is given.
 n - total number of characters in the code (code length),
 k - number of information symbols,
 d - the minimum distance of Heming code combinations;
 g - the genus of the curve,
 degF - degree of generator function,
 degCurve is the degree of curve

Stage 2. Formation of personal and public keys of asymmetric cryptosystem, introduction of information parcel

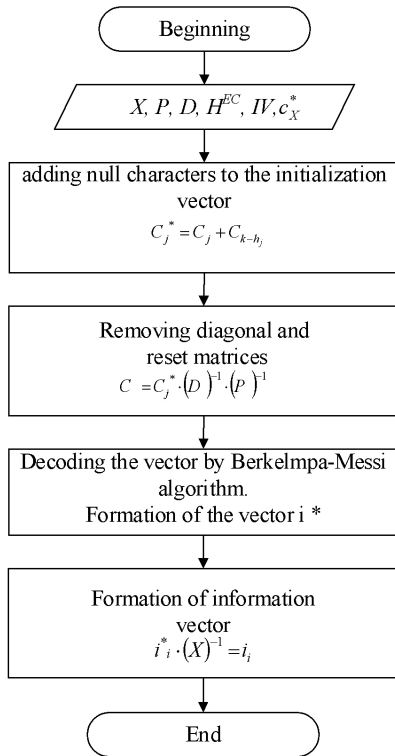
X is a non-degenerate $k \times k$ matrix over $GF(q)$,
 P is a permutational $n \times n$ matrix over $GF(q)$,
 D is the diagonal $n \times n$ matrix over $GF(q)$,
 G^{EC} -generating $k \times n$ matrix of elliptic code $GF(q)$, a_i - set of coefficients of the polynomial of curve $a_1, \dots, a_g$,
 IV - initialization vector, $|IV| = \frac{1}{2}k$ - elements of reduction

Stage 3. Formation of the session key and the codogram

vector e is formed by chance, equally probable and independently from other closed texts

In the communication channel, the code word c_X^* is received without zero elements of the initialization vector (shortening operation)

Fig. 3.6. Algorithm formation codogram in MNCCS McEliece with short MEC



Stage 1. Setting the parameters of the code, entering a personal key and a codec

X is a nondegenerate $k \times k$ matrix over $GF(q)$,
 P is a permutational $n \times n$ matrix over $GF(q)$,
 D is the diagonal $n \times n$ matrix over $GF(q)$,
 H^{EC} – generating $k \times n$ matrix of elliptic code $GF(q)$,
 a_i – set of coefficients of the polynomial of curve
 $a_1 \dots a_6$.

Stage 2. Disassembly codographs

Fig. 3.7. Decoding algorithm in MNCCS McEliece with short MEC

Put in information vector I in a subset of h zeros that is. $I_i = 0, \forall I_i \in h$. On the other positions, I put the vector information symbols. Once in position add the initialization vector information symbols. For modification (extension) will use the elliptical codes set point reduction curve. Fair the following statement.

Statement 8. Let the EC — elliptic curve over $GF(q)$, $g = g(EC)$ — the family of the curve, $EC(GF(q))$ — the set of points over a finite field, $N = EC(GF(q))$ — their number. Fix subset $h_1 \subseteq h$, $|h_1| = x_1$. Let set elliptical (n, k, d) code over $GF(q)$, built through the reflection type $\varphi: X \rightarrow P^{k-1}$. Then extended options for x_1 symbols of $GF(q)$ elliptic code built through the reflection type $\varphi: (X \cup h_1) \rightarrow P^{k-1}$, $n = 2\sqrt{q} + q + 1 - x + x_1$ are related by $k: k \geq \alpha - x + x_1$, $d \geq n - \alpha$, $\alpha = 3 \cdot \deg F$.

Bringing. If $x_1 < x$, then the extension code on x_1 is equivalent to shortening the source code $x - x_1$. Substituting these parameters in expression (3.12), we get the result outcome 1.

Outcome 2. If you know kind of elliptic curve (set $a_1 \dots a_6, \forall a_i \in GF(q)$), the subset h and h_1 fully define modified elliptical (n, k, d) code over $GF(q)$, built through display type: $\varphi: X \rightarrow P^{k-1}$ and $\varphi: (X \cup h_1) \rightarrow P^{k-1}$.

Proof. A set of coefficients $a_1 \dots a_6, \forall a_i \in GF(q)$ specifies the type of elliptic curve and, therefore, a set of dots $EC(GF(q))$. Using the display type $\varphi: EC \rightarrow P^m$ statements and results of 1–2, construct elliptical (n, k, d) code over $GF(q)$. If you know the extension of the characters, the extended build codes. According to the 8 symbols set h_1 , which fully define a modified elliptical (n, k, d) code over $GF(q)$.

Statement 9. Fix subset $h_1 \subseteq h, |h_1| = x_1$. Let set elliptical (n, k, d) code over $GF(q)$, built through the display view $\varphi: X \rightarrow P^{r-1}$. Then extended options for x_1 symbols of $GF(q)$ elliptic code built through the reflection type $\varphi: (X \cup h_1) \rightarrow P^{r-1}$, are related: $n = 2\sqrt{q} + q + 1 - x + x_1, k \geq n - \alpha, d \geq \alpha, \alpha = 3 \cdot \deg F$.

Outcome 3. If you know kind of elliptic curve (set $a_1 \dots a_6, \forall a_i \in GF(q)$), the subset h and h_1 fully define modified elliptical (n, k, d) code over $GF(q)$, built through display type: $\varphi: X \rightarrow P^{r-1}$ and $\varphi: (X \cup h_1) \rightarrow P^{r-1}$.

Proof. A set of coefficients $a_1 \dots a_6, \forall a_i \in GF(q)$ specifies the type of elliptic curve and, therefore, a set of dots $EC(GF(q))$. Using the display type $\varphi: EC \rightarrow P^m$ statements and results 1–2, build elliptical (n, k, d) code over $GF(q)$. If you know the extension of the characters, the extended build codes. According to 9 sets of symbols h and h_1 , which fully define a modified elliptical (n, k, d) code over $GF(q)$.

Results statements 8, 9 and their consequences can build modified (extended within $n \leq 2\sqrt{q} + q + 1$) Elliptical (n, k, d) code over $GF(q)$. Define the following algorithm for constructing modified elongated elliptical codes.

Algorithm elongated elliptical construction codes.

Step 1. Fix elliptic curve over $GF(q)$. We find a set of simple points of the curve $EC(GF(q)): (P_1, P_2, \dots, P_N)$. Construct shortened (n, k, d) code over $GF(q)$ as a result of reflection $\varphi: X \rightarrow P^m$.

Step 2. Fix a subset of points of the curve $h_1(GF(q)): (Rx_1, Rx_2, \dots, Rxx_1), h_1 \subseteq h, |h_1| = x_1$.

Step 3. Construct display $\varphi: (X \cup h_1) \rightarrow P^m$. If $M = k$, we obtain an elongated elliptical (n, k, d) code over $GF(q)$ with parameters $n = 2\sqrt{q} + q + 1 - x + x_1, k \geq \alpha - x + x_1, d \geq n - \alpha, \alpha = 3 \cdot \deg F$ (See Consequently approving 10). If $M = r$, we obtain elongated elliptical (n, k, d) code over $GF(q)$ with the following parameters: $n = 2\sqrt{q} + q + 1 - x + x_1, k \geq n - \alpha, d \geq \alpha, \alpha = 3 \cdot \deg F$.

Using the result 8 statement and its implications ask MNCCS McEliece extended to MEC constructed through mapping species $\varphi: X \rightarrow P^{k-1}$ and $\varphi: (X \cup h_1) \rightarrow P^{k-1}$. Fair the following statement.

Statement 10. An elongated elliptical (n, k, d) code over $GF(2^m)$, built through the reflection type $\varphi: (X \cup h_1) \rightarrow P^{k-1}$ determines MNCCS with parameters:

The dimension of the secret key (in bits):

$$l_{k+} = (x - x_1) \cdot \left\lceil \log_2 (2\sqrt{q} + q + 1) \right\rceil. \quad (3.29)$$

Dimension vector information (in bits):

$$l_i = (\alpha - x + x_1) \cdot m. \quad (3.30)$$

Cryptograms dimension (in bits):

$$l_s = (2\sqrt{q} + q + 1 - x + x_1) \cdot m. \quad (3.31)$$

Relative speed:

$$R = (\alpha - x + x_1) / (2\sqrt{q} + q + 1 - x + x_1). \quad (3.32)$$

Bringing. According to the results statement 10 MNCCS McEliece, built using generative matrix (n, k, d) code over $GF(2^m)$, has the following parameters: the size of the secret key $k \times n$ symbols of $GF(2^m)$; information vector of length k symbols of $GF(2^m)$; length codogram — n symbols of $GF(2^m)$; Relative speed — $R = k/n$. Number the record straight curve. Total of $N \leq 2\sqrt{q} + q + 1$.

So, for numbering the points curve necessary $\left\lceil \log_2 (2\sqrt{q} + q + 1) \right\rceil$ bit. If the power symbol subset shortening $|h| = x$ then to describe all characters need shortening $x \cdot \left\lceil \log_2 (2\sqrt{q} + q + 1) \right\rceil$ bit. These characters are kept in secret and set the amount of key data — expression (3.14). If the power symbol subsets extension $|h_1| = x_1$ then to describe all characters need updating $(x - x_1) \cdot \left\lceil \log_2 (2\sqrt{q} + q + 1) \right\rceil$ bit. These characters are kept in secret and set the amount of key data — expression (3.20).

Using the result 8 statement and its implications ask MNCCS built through the reflection type $\varphi: X \rightarrow P^{r-1}$ and $\varphi: (X \cup h_1) \rightarrow P^{r-1}$. Fair the following statement.

Statement 11. An elongated elliptical (n, k, d) code over $GF(2^m)$, built through the reflection type $\varphi: (X \cup h_1) \rightarrow P^{r-1}$ determines MNCCS with parameters:

Private key dimension is defined by (3.29);

Dimension vector information (in bits):

$$l_i = (2\sqrt{q} + q + 1 - \alpha) \cdot m. \quad (3.33)$$

Codogram dimension is defined by (3.31);

Relative speed:

$$R = (2\sqrt{q} + q + 1 - \alpha) / (2\sqrt{q} + q + 1 - x + x_1). \quad (3.34)$$

Bringing. According to the results statement 2 NCCS built using matrix algebraic checking block (n, k, d) code over $GF(2^m)$, has the following parameters: a vector of length k information symbols of $GF(2m)$; length codogram — n symbols of $GF(2^m)$; Relative speed — $R = k/n$. Substituting the parameters modified (shortened and elongated) elliptical (n, k, d) code over $GF(q)$, built through the reflection type $\varphi: X \rightarrow P^{r-1}$ and $\varphi: (X \cup h_1) \rightarrow P^{r-1}$ (see 9 statements) receive, respectively, expression (3.33) (3.34).

Thus, the results statements 8, 9 and their consequences can build modified elongated elliptical (n, k, d) code over $GF(q)$. Statements 10 and 11 allow you to specify MNCCS McEliece for MEC, thus providing the necessary cryptographic immunity.

Consider formal description MNCCS information security through the use of methods of modification.

Mathematical model modified asymmetric crypto-code information protection system using geometrical block codes based MNCCS McEliece-based extension (increase information symbols) formally given the totality of the following elements:

– A set of open-source: $M = \{M_1, M_2, \dots, M_{q^k}\}$, where $M_i = \{I_0, I_{h_1}, \dots, I_{h_j}, I_{k-1}\}$,

$\forall I_j \in GF(q), H_j$ — information symbols are zero, $|h| = \frac{1}{2}k$ i.e. $I_i = 0, \forall I_i \in h; h_r$ —

extension of information symbols $k, |h| = \frac{1}{2}k$;

– Closed set of texts (codogram):

$C = \{C_1, C_2, \dots, C_{q^k}\}$, where $C_i = (c_{X_0}^*, c_{h_1}^*, \dots, c_{h_j}^*, c_{X_{n-1}}^*), \forall c_{X_j}^* \in GF(q)$;

– Set direct mappings (based on the use of public key — generative matrix): $\phi = \{\phi_1, \phi_2, \dots, \phi_s\}$, where $\phi_i: M \rightarrow C_{h_r}, i = 1, 2, \dots, s$;

– Set of inverse mapping (through the use of closed (private) key — masking matrix): $\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, \dots, \phi_s^{-1}\}$, where $\phi_i^{-1}: C_{h_r} \rightarrow M, i = 1, 2, \dots, s$;

– A set of keys that parameterize direct reflection (public key authorized user): $K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, \dots, K_{s_{a_i}}\} = \{G_{X_{a_i}}^{EC_1}, G_{X_{a_i}}^{EC_2}, \dots, G_{X_{a_i}}^{EC_s}\}$,

where $G_{X_{a_i}}^{EC_i}$ — generative $k \times n$ Matrix disguised random code block geometrical (n, k, d) with elements of the code $GF(q)$ that is $\phi_i: M \xrightarrow{K_{ia_i}} C_{hr};$

$i = 1, 2, \dots, s$;

– A_i — a set of polynomial curve coefficients $a_1 \dots a_6$, $\forall a_i \in GF(q)$ clearly poses a specific set point curve space P^2 .

A set of keys that parameterize reverse mapping (private (secret) key authorized user)):

$$K^* = \{K_1^*, K_2^*, \dots, K_s^*\} = \{\{X, P, D\}_1, \{X, P, D\}_2, \dots, \{X, P, D\}_s\},$$

$$\{X, P, D\}_i = \{X^i, P^i, D^i\}, \quad (3.35)$$

where X^i — masking nondegenerate randomly generated equally probable source keys $k \times k$ matrix elements of $GF(q)$; P^i — rearrangement randomly generated equally probable source keys $n \times n$ matrix elements of $GF(q)$. D^i — diagonal formed a key source $n \times n$ matrix elements of $GF(q)$, that is — $\phi_i^{-1} : C \xrightarrow{K_i^*} M$, $i = 1, 2, \dots, s$, the complexity of reverse mapping ϕ_i^{-1} without knowledge of the key $K_i^* \in K^*$ related to the decision-theoretic challenger — decoding the random code (code common position).

Initial data in the description are considered NCCS options in previous models.

In MNCCS McEliece modified (extended) geometrical (n, k, d) code C_{h_r} with fast decoding algorithm disguised as random (n, k, d) code $C_{h_r}^*$ by multiplying generative matrix GES code C_{k-h_j} masking the matrix stored in a secret X^u , P^u and D^u , to form the public key of the authorized user:

$$G_X^{ECu} = X^u \cdot G^{EC} \cdot P^u \cdot D^u, \quad u \in \{1, 2, \dots, s\}, \quad (3.36)$$

where G^{EC} — generative matrix block geometrical (n, k, d) with elements of the code $GF(q)$ built on the basis of user-selected polynomial curve coefficients $a_1 \dots a_6$, $\forall a_i \in GF(q)$ clearly define a specific set point curve space P^2 .

Forming a closed text $C_j \in C_{h_r}$ entered in clear text $M_i \in M$ and given public key $G_X^{ECu_{a_i}}$, $u \in \{1, 2, \dots, s\}$ carried out by forming a shortened codeword, and then disguised extension of the code of adding to it randomly generated vector $e = (e_0, e_1, \dots, e_{n-1})$:

$$C_j = \phi_u(M_i, G_X^u) = M_i \cdot (G_X^u)^T + e. \quad (3.37)$$

For each molded 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 that is formed by accident, equally probable and closed independently of the other texts.

In the channel coming $C_j^* = C_j - C_{k-h_j} + C_{h_r}$.

On the receiving side, the authorized user who knows masking rule, the number and location information null characters can use speed decoding algorithm geometrical code (polynomial complexity) to recover the plaintext:

$$M_i = \phi_u^{-1}(C_j^*, \{X, P, D\}_u). \quad (3.38)$$

To restore the plaintext authorized user replaces characters elongation at zero information symbols:

$$C_j^* = C_{h_r} \rightarrow C_{k-h_j}. \quad (3.39)$$

Recovered from a closed text C_j takes effect rearrangement and secret diagonal matrix P^u and D^u :

$$\begin{aligned} C &= C_j^* \cdot (D^u)^{-1} \cdot (P^u)^{-1} = (M_i \cdot (G_X^u)^T + e) \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \\ &= (M_i \cdot (X^u \cdot G \cdot P^u \cdot D^u)^T + e) \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \\ &= M_i \cdot (X^u)^T \cdot (G)^T \cdot (P^u)^T \cdot (D^u)^T \cdot (D^u)^{-1} \cdot (P^u)^{-1} + e \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \\ &= M_i \cdot (X^u)^T \cdot (G)^T + e \cdot (D^u)^{-1} \cdot (P^u)^{-1}. \end{aligned} \quad (3.40)$$

Decode received vector algorithm Berlekempa-Messi:

$$C = M_i \cdot (X^u)^T \cdot (G^{EC})^T + e \cdot (D^u)^{-1} \cdot (P^u)^{-1}. \quad (3.41)$$

That gets rid of the second term and the multiplier $(G)^{ECT}$ in the first term on the right side of equality, then remove the masking effect of the matrix X^u .

For the result of decoding M_i^* be multiplied by $(X^u)^{-1}$:

$$M_i^* \cdot (X^u)^{-1} = M_i. \quad (3.42)$$

The resulting solution — plain text M_i To which characters are added extension: $M_j = M_i + h_r$ — are transmitted message.

Block diagram of protocol information in real time using asymmetric cryptosystem based MNCCS McEliece with modified (extended) elliptical codes shown in Fig. 3.8.

Fig. 3.9 The algorithm encoding MNCCS McEliece extended to MEC, decoding algorithm shown in Fig. 3.10.

To assess the time and speed performance commonly used unit cpb, where cpb (cycles per byte) — the number of cycles of the processor that need to spend for processing one byte of input. The complexity of the algorithm is calculated by the expression: $Per = Utl * CPU_clock / Rate$, where Utl — utilization of processor cores (%), $Rate$ — bandwidth algorithm (bytes/sec).

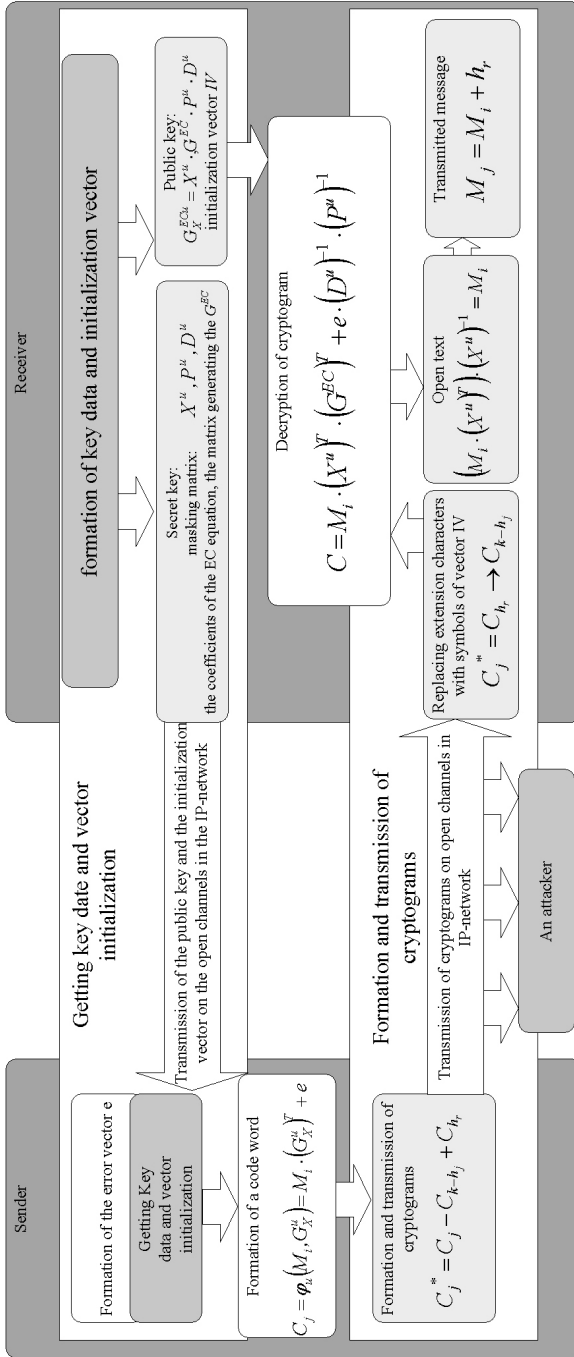
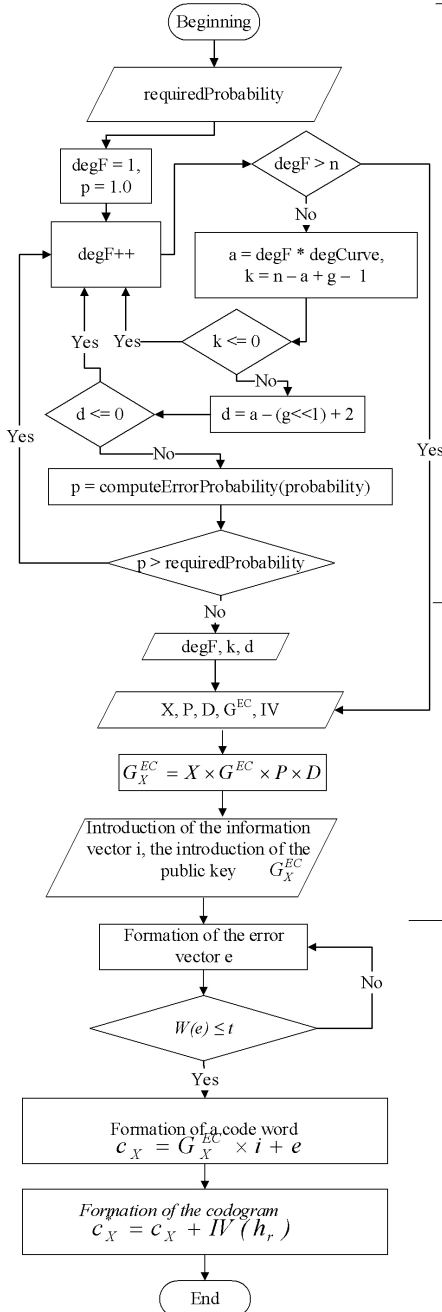


Fig. 3.8. Protocol to exchange information in real time from MEC MNCCS



Stage 1. Setting the code parameters

Required Probability - The probability of block distortion is given.

n - The total number of characters in the code (code length),

k - number of information symbols,

d - the minimum distance of Heming code combinations;

g - the genus of the curve,

$\deg F$ - degree of generator function,

$\deg \text{Curve}$ is the degree of curve.

Stage 2. Formation of personal and public keys of asymmetric cryptosystem, introduction of information parcel

X is a nondegenerate $k \times k$ matrix over $GF(q)$,

P is a permutational $n \times n$ matrix over $GF(q)$,

D is the diagonal $n \times n$ matrix over $GF(q)$,

G^{EC} - generating $k \times n$ matrix of elliptic code over $GF(q)$,

a_i - set of coefficients of the polynomial of curve $a_1 \dots a_g$

IV - initialization vector, $|IV| = \frac{1}{2} k$ - elements of reduction

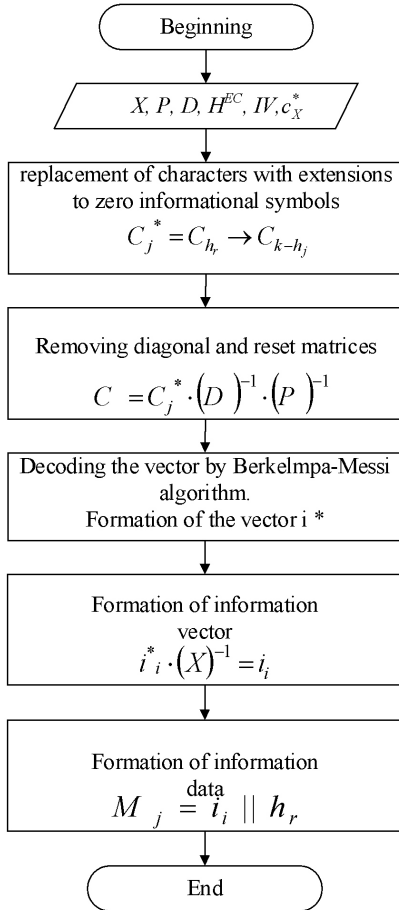
h_r - extensions, $|h_r| = \frac{1}{2} k$

Stage 3. Formation of the session key and the codogram

Vector e is formed by chance, equally probable and independently from other closed texts

A communication code enters the communication channel with the insertion of zero elements of the vector of initialization of non-zero elements of information symbols (elongation operation)

Fig. 3.9. Algorithm formation codogram in MNCCS McEliece extended to MEC



Stage 1. Setting the parameters of the code, conducting a private key and codogram

X is a nondegenerate $k \times k$ matrix over $GF(q)$, P is a permutational $n \times n$ matrix over $GF(q)$, D is the diagonal $n \times n$ matrix over $GF(q)$, NEC -verifiable $r \times n$ matrix of the elliptic code over $GF(q)$, ai - set of coefficients of the polynomial of the curve $a_1 \dots a_6$, IV - initialization vector, $IV = |h| = \frac{1}{2}k$ - elements of reduction

Stage 2. Decoding the codogram

Stage 3. Formation of information data

Information data is formed on the basis of the algorithm of concatenation of the information vector and the characters of the extension. In the event of an error in the extension symbols, a codeword consisting of n symbols with null elements supplemented with extensions is generated and the Berkelampa algorithm is used to restore them.

Fig. 3.10. Decoding algorithm in codogram MNCCS McEliece

Table 3.7, 3.8, 3.9, 3.10 these results depending on the length of the code sequence MEC (shortened/lengthened) in MNCCS McEliece on the number of CPU cycles to perform basic operations software implementation crypto-code systems.

Analysis Table 3.7, 3.8, 3.9, 3.10 shows that the use of modified (shortened/lengthened) MEC reduces the energy capacity of program implementation MNCCS McEliece almost 2 times, but to provide the required level of reliability in the implementation of smaller field $GF(2^6-2^8)$. Consider the basic properties of the modified proposed cryptosystem (cryptoconversions speed, complexity break and so on).

Table 3.7. — Research results depending on the length of the code sequence in MNCCS McEliece shortened to MEC on the number of CPU cycles

The length of the code sequence		McEliece to shortened codes			McEliece		
		10	100	1000	10	100	1000
Number of function calls that implement basic operations	Reading symbol	10294397	28750457	76759874	11018042	30800328	80859933
	Comparing strings	3406921	9246748	25478498	3663356	10199898	26364634
	Concatenation line	1705544	5045748	12379422	1834983	5125564	13415329
* Duration of functions in processor cycle	Sum	15406862	43042953	114617794	16516381	46125790	20639896
	Reading symbol	295374	810478	2001167	297487	831609	2183218
	Comparing strings	178814	531379	1248684	197821	550794	1423690
Sum	Concatenation line	544990	1328114	3586486	544990	1522293	3984353
		1006781	2749548	7247488	1040298	2904696	7591261
Duration performance ** in ms		0.52	1.37	3.4	0.55	1.53	4

Note:

* The 1000 operations per processor cycle: reading character — 27 cycles, comparing lines — 54 cycles string concatenation — 297 cycles;

** taken for calculating processor clocked at 2 GHz based operating system 5 %.

Table 3.8. — Research results evaluation time and speed performance procedures for forming and decoding information in MNCCS truncated at MEC

Indexes	The length of the code sequence	The capacity of the algorithm, Rate, (bytes/s)	Recycling processor cores (%)	The complexity of the algorithm, Per (cpb)
Number of function calls that implement basic operations	100	46125790	56	61.5
	1000	120639896	56	62.0

Table 3.9. — Research results depending on the length of the code sequence in MNCCS McElice extended to MEC on the number of CPU cycles

Length code sequence	McElice for extended codes			McElice		
	10	100	1000	10	100	1000
Number of function calls that implement basic operations	Reading symbol	11432131	33460317	82473442	11018042	30800328
	Comparing strings	3673756	121119867	29469389	3663356	10199898
	string concatenation	1947681	6114478	14456729	1834983	5125564
Sum		17053568	51694662	126399560	16516381	46125790
* Duration of functions in processor cycle	Reading symbol	300479	843705	2745148	297487	831609
	Comparing strings	213478	561754	1739170	197821	550794
	string concatenation	578174	1647638	4007883	544990	1522293
Sum		109157	1092131	3053097	1040298	2904696
Duration of ** in ms		0.56	1.55	4.1	0.55	1.53
						4

Note: * — The 1000 operations per processor cycle: reading character — 27 cycles, comparing lines — 54 cycles string concatenation — 297 cycles;

** — taken for calculating processor clocked at 2 GHz based operating system 5 %.

Table 3.10. — Research results evaluation time and speed performance procedures for forming and decoding information

Indexes	The length of the code sequence	The capacity of the algorithm, Rate, (bytes/s)	Recycling processor cores (%)	The complexity of the algorithm, Per (cpb)
NCCS McElice in EC	100	46125790	56	61.5
	1000	120639896	56	62.0
IAMB macro Elisa at MEC	100	51694662	56	61.7
	1000	126399560	56	62.2

3.1.4 Research on properties of modified elliptical cryptographic codes

A comparative evaluation parameters NCCS McEliece on *EC* MNCCS using modified elliptical codes. We introduce the following notation:

l_i — the length of the sequence information (block), which is the input of the CCS scheme (in bits); l_k — public key length (in bits); l_{k+} — private key length (in bits); l_s — codogram length (in bits); O_k — forming codogram complexity (number of group operations); O_{sk} — complexity decoding codogram (number of group operations); O_{k+} — the complexity of solving the problem analysis (the number of group operations). For charting used conventional reduction (console): uk — MNCCS with short MECs; ud — MNCCS with a long month. In calculating parameters cryptosystems used Galois field: for TCS McEliece — $GF(2^{10})$; for MNCCS with short/extended MEC — $GF(2^6)$.

To estimate the length of sequence information (in bits) that receives input from MES MNCCS (n, k, d) — code over $GF(2^m)$ use the expression:

TCS for the *EC*: $l_i = k \times m$;

MNCCS for *MEC* on the truncated codes: $l_i = 1/2k \times m$;

MNCCS for an extended *MEC* codes: $l_i = k \times m$.

Table 3.11 in Fig. 3.11 are depending on the complexity of forming codogram the power off.

Table 3.11. — Dependence difficulty forming cryptograms in different $GF(2^m)$

$GF(2^m)$	Relative encoding rate, R					
	0.5	0.75	0.5(<i>ud</i>)	0.75(<i>ud</i>)	0.5(<i>uk</i>)	0.75(<i>uk</i>)
3	31	87	242	603	817	968
4	76	340	760	980	2140	6282
5	335	872	2241	6121	8706	11461
6	582	2170	6348	9830	10722	60760
7	1023	6172	17092	61751	83000	210170
8	5237	10673	67016	105265	207422	605005
9	10563	50487	98765	510780	710920	1018079
10	52704	103822	497309	908243	4572881	5561379

These data show that the complexity of forming cryptograms to the selected power Galois field 2^6 on the truncated and extended codes is much lower (5 times more) than the original implementation at TAS *EC*. Accordingly, the rate of formation of cryptograms significantly increased.

To evaluate codogram length (in bits) use the expression:

TCS for the *EC* to: $l_s = n \times m$;

for MNCCS truncated at *MEC*: $l_s = (2\sqrt{q} + q + 1 - 1/2k) \times m$;

MNCCS extended for at MEC: $l_s = \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times m$.

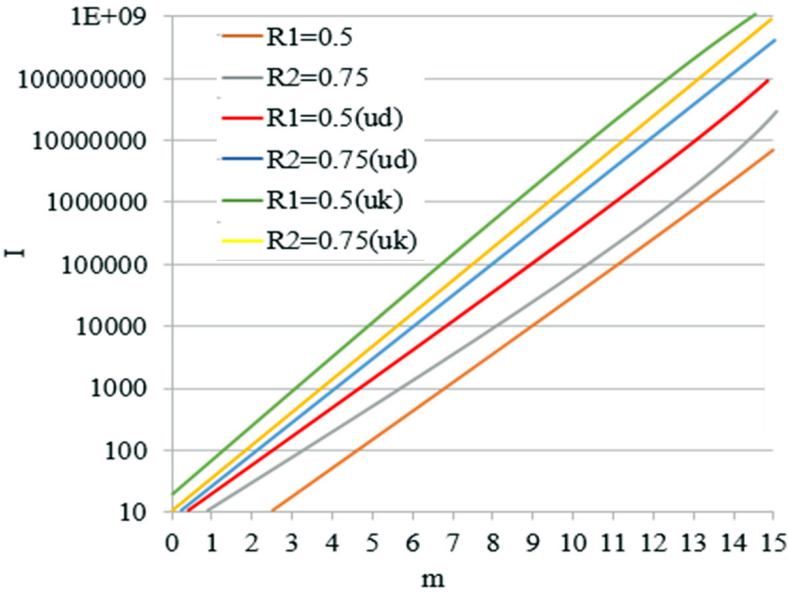


Fig. 3.11. Dependence difficulty forming cryptograms in different $GF(2^m)$

Table 3.12 and Fig. 3.12 decoding complexity are dependent on the power codogram field.

Table 3.12. — Dependencies decoding complexity
codogram the power field $GF(2^m)$

$GF(2^m)$	R					
	0.5	0.75	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)
1	43	57	78	81	82	96
2	67	98	456	457	457	556
3	120	640	1024	1168	1280	5127
4	680	2378	7672	8232	11028	23674
5	2092	7512	21073	42082	78634	277830
6	12397	61246	103862	281472	760553	5220573
7	127523	136495	642648	752018	4566721	19768512
8	1203984	1494284	3564898	3957812	12948312	52694229
9	10637991	12768954	54678128	67458242	92516734	102564872
10	175645127	193648924	1e + 09	1e + 09	1e + 09	1e + 09

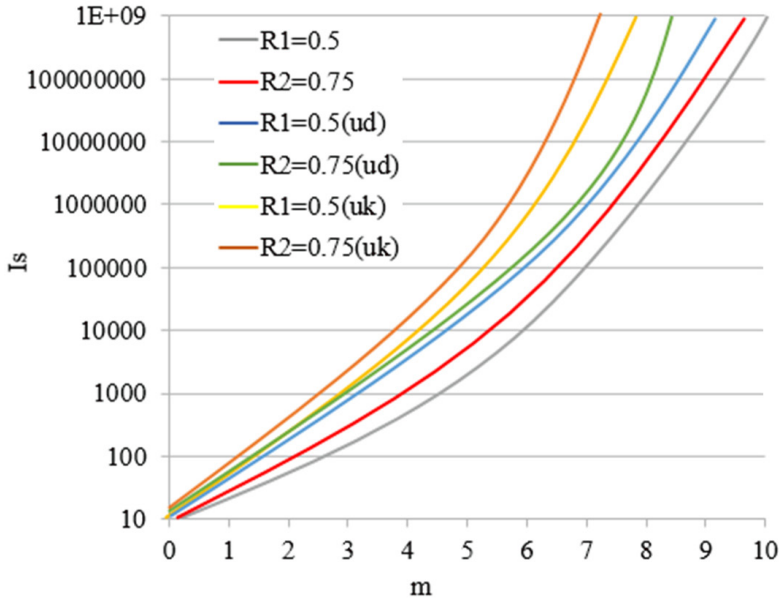


Fig. 3.12. Dependence difficulty decoding cryptograms in different $GF(2^m)$

Analysis of calculation as well as in the case of forming cryptograms, shows a significant increase decoding speed using shortened and elongated months.

Public key length (in bits) the sum of matrix elements $G G_X^{EC}$ and is given by the expressions:

TCS for the EC to: $l_K = k \times n \times m$;

for MNCCS truncated at MEC: $l_K = 1/2k \times (2\sqrt{q} + q + 1 - 1/2k) \times m$;

MNCCS extended for at MEC: $l_K = 1/2k \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k) \times m$.

The length of the secret key (In bits) is the sum of matrix elements X, P, D (in bits), and is given by the expressions:

TCS for the EC to: $l_{K+} = n_2 \times k_2 \times m$;

for MNCCS truncated at MEC: $l_{K+} = 1/2k \left[\log_2 (2\sqrt{q} + q + 1) \right]$,

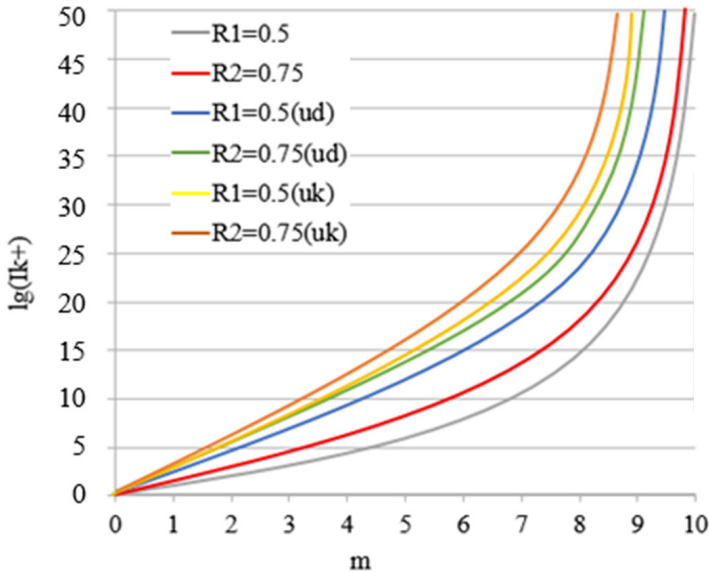
MNCCS extended for at MEC: $l_{K+} = (1/2k - 1/2k) \left[\log_2 (2\sqrt{q} + q + 1) \right]$.

Table 3.13 in Fig. 3.13 are depending on the complexity of breaking through rearrangement decoding the power off.

Analysis Fig. 3.13 showed that reducing the capacity of the field to 26 did not lead to a significant reduction in complexity by breaking cryptograms Adjustable decoding.

Table 3.13. — Dependence difficulty breaking in different $GF(2^m)$

$GF(2^m)$	R					
	0.5	0.75	0.5(<i>ud</i>)	0.75(<i>ud</i>)	0.5(<i>uk</i>)	0.75(<i>uk</i>)
1	1.056	1.38	2.786	2.835	4.122	4.257
2	2.237	3.017	4.978	5.961	6.233	6.781
3	2.868	4.867	7.568	8.120	8.234	9.764
4	4.843	6.613	9.87	12.1	12.647	13.32
5	6.22	8.03	12.017	14.224	14.742	16.892
6	7.891	12.245	14.983	17.483	18.767	19.76
7	8.995	13.13	17.14	20.32	21.102	22.93
8	10.37	15.16	19.55	23.23	24.05	26.11
9	11.74	17.18	21.96	26.15	27.002	29.302
10	13.19	19.23	24.37	29.06	29.95	32.484

Fig. 3.13. Dependence difficulty breaking in different $GF(2^m)$
(Adjustable decoding)

Difficulty forming codogram estimated expressions:

For the TCS to the EC: the implementation of a systematic coding:

$$O_K = (r+1) \times n; \text{ for non-systematic coding: } O_K = (k+1) \times n.$$

For MNCCS truncated at MEC: the implementation of a systematic coding:

$$O_K = (r+1) \times (2\sqrt{q} + q + 1 - 1/2k). \quad (3.43)$$

For non-systematic coding:

$$O_K = (k+1) \times (2\sqrt{q} + q + 1 - 1/2k). \quad (3.44)$$

For MNCCS extended to MEC: the implementation of a systematic coding:

$$O_K = (r+1) \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k). \quad (3.45)$$

For non-systematic coding:

$$O_K = (k+1) \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k). \quad (3.46)$$

The difficulty decoding codogram determined by the expressions:

TCS for the EC to:

$$O_{SK} = 2 \times n^2 + k^2 + 4t^2 + (t^2 + t - 2)^2/4;$$

for MNCCS truncated at MEC:

$$O_{SK} = 2 \left(2\sqrt{q} + q + 1 - 1/2k \right)^2 + 1/2k^2 + 4t^2 + (t^2 + t - 2)^2/4. \quad (3.47)$$

MNCCS extended for at MEC:

$$O_{SK} = 2 \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k \right) + k^2 + 4t^2 + (t^2 + t - 2)^2/4. \quad (3.49)$$

The complexity of the task analysis (decoding) asked expressions:

TCS for the EC to:

$$O_{K+} = N_{coating} \times n \times r, \quad (3.50)$$

$$\text{where } N_{coating} \geq \frac{C_n^{\rho \cdot t}}{C_{n-k}^{\rho \cdot t}} = \frac{n(n-1) \dots (n - \rho \cdot t - 1)}{(n-k)(n-k-1) \dots (n-k - \rho \cdot t - 1)}, \quad t = \lfloor (d-1)/2 \rfloor.$$

Potential resistance cryptosystem is determined by $\rho \times t$, and the stability of the system — $(1 - \rho) \times t$.

For MNCCS to shortened codes:

$$O_{K+} = N_{coating} \times (2\sqrt{q} + q + 1 - 1/2k) \times r. \quad (3.51)$$

MNCCS for an extended codes:

$$O_{K+} = N_{coating} \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k) \times r. \quad (3.52)$$

Table 3.14 and Fig. 3.14 are depending on the complexity and difficulty of breaking coding for different velocities EC (MEC).

Table 3.15 in Fig. 3.15 are the dependence of public key data for different indicators of sustainability.

Analysis of the results table 3.14, 3.15, Fig. 3.14, 3.15 clearly demonstrates thereby obtained relative increase in the data rate, the amount of key data systems for shortened/lengthened half the usual codes NCCS.

Table 3.14. — Overall chart fracture complexity and difficulty of coding for different velocities EC

$\lg(l_s)$	0.5	0.75	0.5(<i>ud</i>)	0.75(<i>ud</i>)	0.5(<i>uk</i>)	0.75(<i>uk</i>)
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

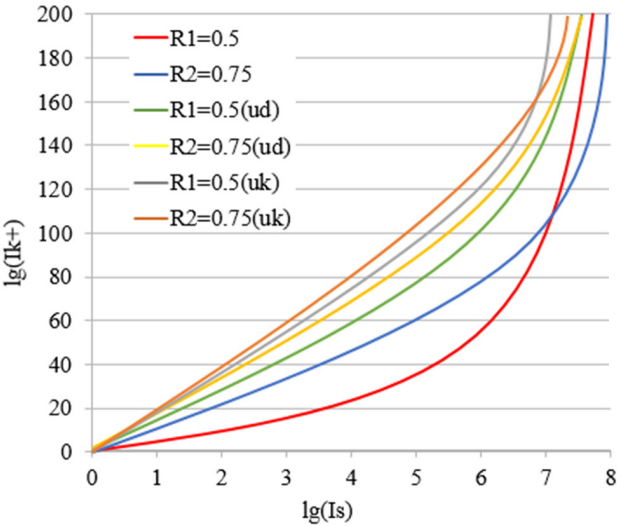


Fig. 3.14. Overall chart fracture complexity and difficulty of coding for different velocities EC(MEA)

Table 3.15. — Dependence of public key data for different indicators of sustainability

$\lg(l_{k+})$	<i>R</i>					
	0.5	0.75	0.5(<i>ud</i>)	0.75(<i>ud</i>)	0.5(<i>uk</i>)	0.75(<i>uk</i>)
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

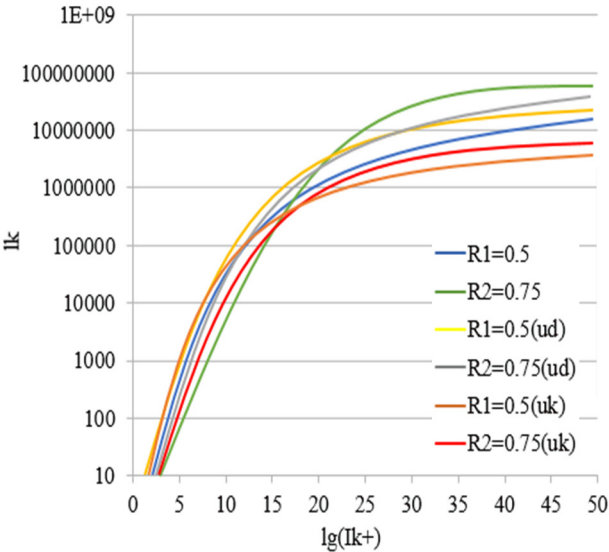


Fig. 3.15. Dependence of public key data for different indicators of sustainability

Table 3.16 These results capacitive characteristics in program implementation capacity of the field.

Table 3.16. — Dependence of software implementation of the power field (Number of group operations)

Crypto-systems	2 ⁵	2 ⁶	2 ⁷	2 ⁸	2 ⁹	2 ¹⁰
NCCS MacElis in <i>EC</i>	10018042	18048068	32847145	47489784	63215578	82467897
MNCCS MacElis trun- cated at <i>MEC</i>	10007947	17787431	28595014	44079433	61974253	79554764
MNCCS MacElis extended to <i>MEC</i>	11156138	18561228	33210708	48297112	65171690	84051337

Results Table 3.16 shows the number of group operations software implementation NCCS depending on the power field. It is evident that if the imple-

mentation NCCS McEliece in field 2^{10} necessary 82.5×10^6 group operations, the implementation MNCCS on shortened/lengthened *MEC* in the field requires $2^6 - 17.7-18.6 \times 10^6$ group operations, i. e. 4.5 times less.

Consider further reduction of energy losses in the practical implementation MNCCS McEliece and Niederreiter be proposed in the next section.

3.2 Develop methods to ensure the integrity and confidentiality of banking information in automated banking systems on hybrid designs crypto code of unprofitable codes

3.2.1 Research on the cryptographic properties of building codes unprofitable

To provide basic services in the security SI ABS in the face of rising threats IS, CB, SI offered TZZI ABS hybrid crypto-code constructions based on the synthesis MNCCS McEliece and Niederreiter on *MEC* and unprofitable codes multichannel cryptography.

In [40, 41] the theoretical and practical bases of unprofitable codes. During flawed text refers to the text obtained by further deformation nonredundant code letters [39].

Thus, a necessary and sufficient condition for the loss of loss of sense of the text is shorter text character codes outside of their excesses. As a result, waning text has a length less than the length of the source text, and no sense of the source text [40].

The theoretical basis for constructing texts are unprofitable ordering the removal of symbols of the source text and therefore reduce redundancy symbols of language in the text unprofitable.

The amount of information that expresses this ordering, equal decrease in entropy of the text compared with the maximum possible entropy, that is equally probable occurrence of any letters after any previous letter. Methods of calculating the information offered in [46] reveal the ratio of provided (that is formed with the prescribed rules) information and the number of unexpected information that you can not foresee. Redundancy text is determined by the expression:

$$B(M) = B_A L_0 = \left(\log N - \frac{H(M)}{L_0} \right) \times L_0, \quad (3.53)$$

where: M — the source; B — redundancy language: $B = R - r$; R — redundancy speech: $R = \log N$; N — power alphabet, r — entropy language one character: $r = H(M) / L$; L — M message length in characters language); $H(M)$ — entropy (uncertainty) message; L_0 — message length N symbols of language content; B_A — redundancy language.

For unprofitable text (FTC) and losses (DSH) using the method of “ideal” compression after m cycles mechanism of injury to C_m [40, 41].

The number of cycles needed to reduce the length of the original text is:

$$m) \frac{\log n - B_A}{\log \eta}, \quad (3.54)$$

where n — the symbol representing power source text;

B_A — redundancy speech;

η — shorter times in the original text MV2 each step (a constant factor).

Quantitative measure of efficiency is the degree of damage to the destruction of meaning, that is the difference entropies unprofitable text and source code in different lengths unprofitable segments of text:

$$d = H(FTC) - \sum_{i=1}^s H(M_i) p_i, \quad \sum_{i=1}^s p_i = 1, \quad s = \left\lceil \frac{L_0 - L_{FTC}}{L_{FTC}} \right\rceil, \quad (3.55)$$

where M_i — part of the source code corresponding to the i -th segment, P_i — its probability, L_0 — M_i length equal to the length of LFTC — unprofitable text, s — number of segments.

For ergodic source symbols of the source text:

$$d_{max} = \log L_{FTC} - H(M_i). \quad (3.56)$$

Fig. 3.16 shows a block diagram of one step universal mechanism of injury.

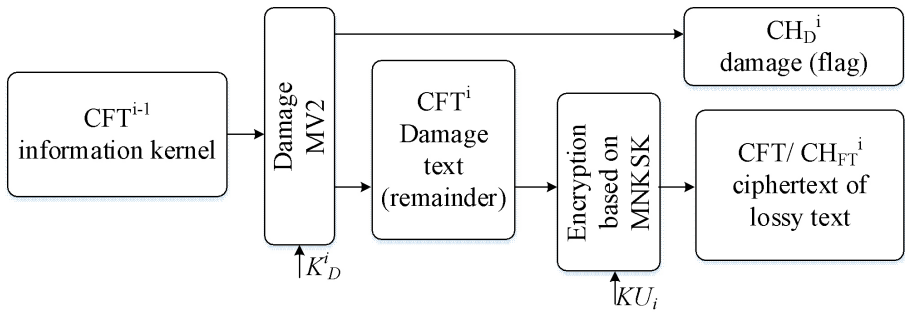


Fig. 3.16. The block diagram of one-step universal mechanism causing damage

Under the information nucleus of some unprofitable text refers to text CFT received cyclic transformation universal mechanism of damage C_m .

The universal mechanism of damage C_m can be described [40, 41]:

$$\begin{aligned} CFT / CH_{FT} &= E_1(M, KU^{EC}), \\ CHD / CH_D &= E_2(M, KU^{EC}), \\ M &= E_{1,2}^{-1}(CFT / CH_{FT}, CHD / CH_D, KU^{EC}), \end{aligned} \quad (3.57)$$

where:

$$\begin{aligned}
 CFT / CH_{FT} &= CFT / CH_{FT}^i, \dots, CFT / CH_{FT}^m, \\
 KU^{EC} &= \varphi(K_D^i, \dots, K_D^m, KU_I^{EC}, \dots, KU_m^{EC}, \\
 CHD / CH_D &= CHD / CH_D^i, \dots, CHD / CH_D^m.
 \end{aligned} \tag{3.58}$$

So as a result we have two ciphertext (loss (SHD) and unprofitable text (FTC)), each of which has no alphabet meaning of the original text, nor ciphertext alphabet. In fact ciphertext original message (M) is represented as a set of two unprofitable ciphertext, each of which individually can not restore the original text.

To restore the original sequence no need to know unprofitable interim order. Need to know only the final sequence of loss-making (the latest unprofitable text after all cycles) and all damages to the rules of their application. The main methods of damage shown in Fig. 3.17, Fig. 3.18 shows the main protocols providing security services through the use of loss-making codes.

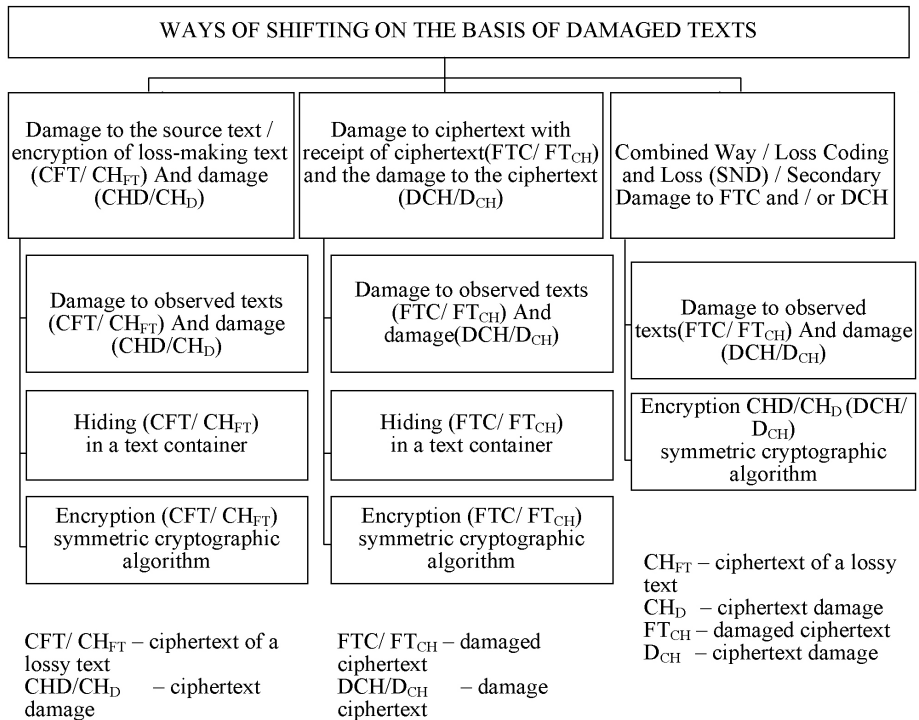


Fig. 3.17. The main methods of damage

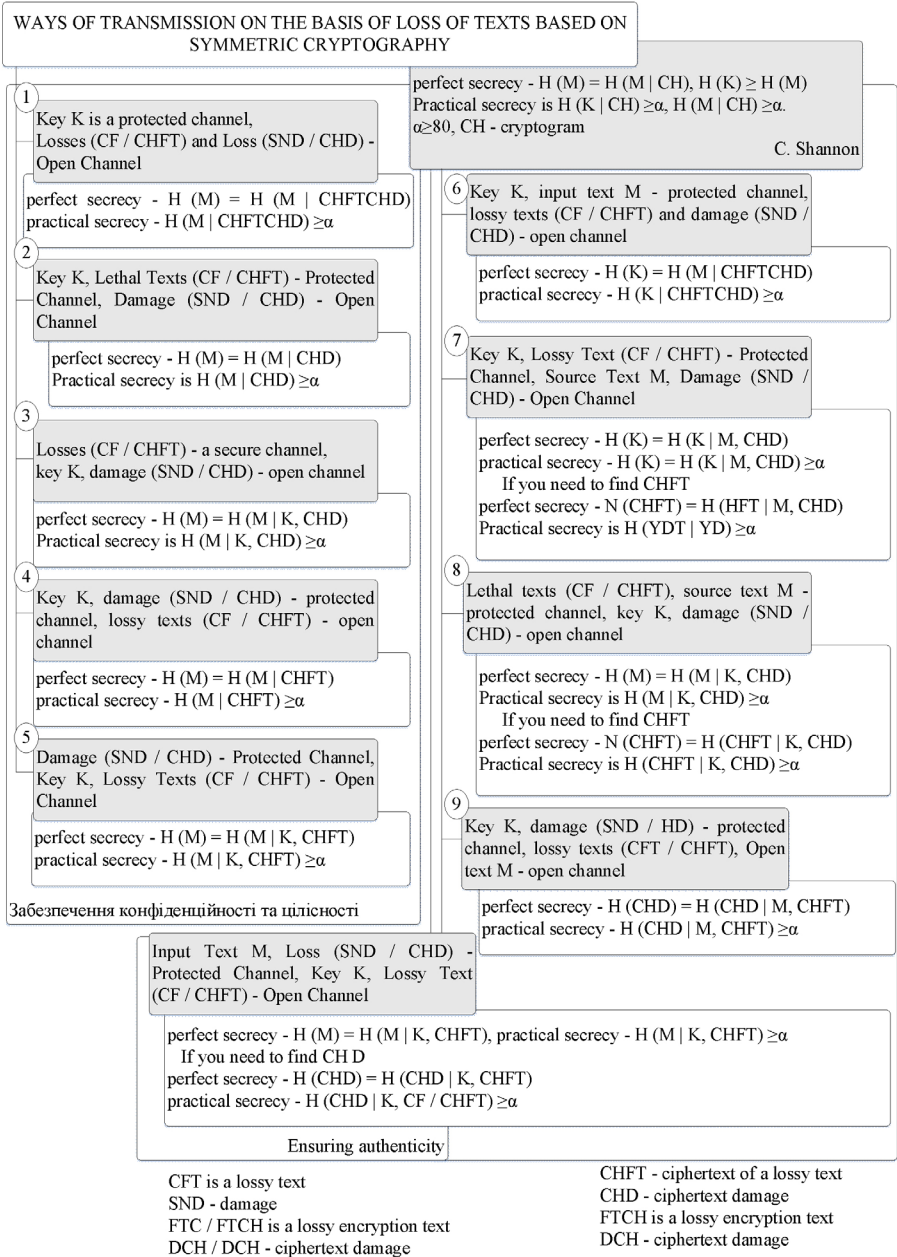


Fig. 3.18. Basic protocols providing security services

Cryptographically flawed texts referred to texts obtained in the following ways [40]:

- damage to the original text, followed unprofitable encrypted text and/or losses;
- damage ciphertext;
- damage ciphertext unprofitable text and/or ciphertext losses.

The main advantage of the proposed methods and protocols providing security services through the use of unprofitable codes are not used BSC and MNCCS McEliece and Niederreiter to ensure cryptographic immunity damage and/or loss-making text.

Distance unity model random cipher for which there is likely to get meaningful text at random and equiprobable selection key K , and attempt to decrypt the ciphertext, the $N_s = H(K) \frac{2^{HL}}{|I|^L} = 1$:

$$L = U_0 = \frac{H(K)}{\log|I| - H} = \frac{H(K)}{B \log|I|}, \quad (3.59)$$

where B — the redundancy of the original text; N — the letter entropy meaningful text in the input alphabet I , $|I| > 2$, 2^{HL} — the approximate value of the number of meaningful texts.

In [40, 41] under cyclic algorithm receiving text refers unprofitable universal mechanism of damage (C_m , where m — number of cycles), which is replacing the random bit representation of each character of the source text tuple or less equal number of bits with further concatenation.

Fig. 3.19 the universal mechanism of damage (MV2 algorithm (forming unprofitable text)). Domain of the transformation algorithm MV2 — set $\{0, 1\}^n$ — alphabet consider a power source of a family, which is associated a probability distribution of letters AZ, and the characters of the source text — the value of discrete random element [40]. Let X — random discrete element that takes value $x_i \in \{0, 1\}^n$ with probability p_i and $T = (c, f) \in F_n^r$ — arbitrary fixed conversion MV2.

Then for any $y \in U_{r, n-1}$ (A binary string of variable length set of lines) and for any $1 \leq i \leq |y|$ performed:

$$\#\{x \in \{0, 1\}^n : c(x) = y\} = \#\{x \in \{0, 1\}^n : c(x) = y^{(i)}\}. \quad (3.60)$$

Then, regardless of the probability distribution of the random element X entropies for random elements $FTC/FTCH$ (unprofitable ciphertext) and CHD (loss) carried equality:

$$H(FTC / FT_{CH}) \leq \log(2^n - 2^r), H(CHD) \leq \log(n - r + 1). \quad (3.61)$$

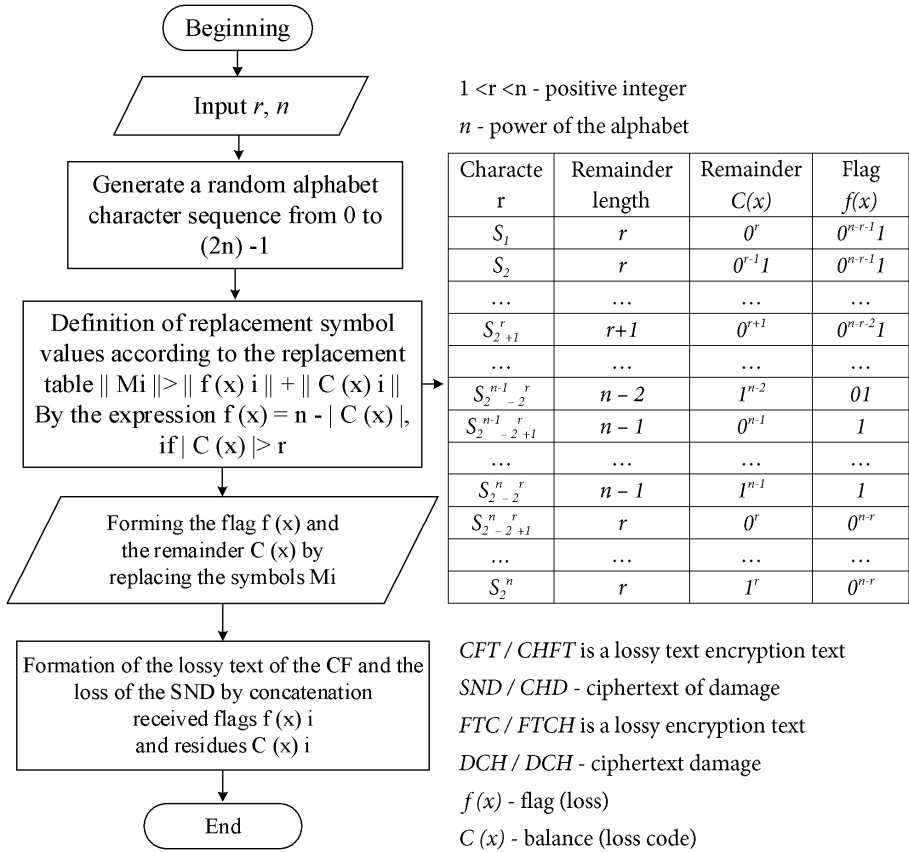


Fig. 3.19. The universal mechanism of damage – algorithm MV2 (formation unprofitable text)

Thus, the uniform distribution of inputs (flag) algorithm MV2 formed even distribution of output (balance):

$$P(c_k = 0 | 0 \leq k \leq |FTC / FT_{CH}|) = \frac{1}{2}. \quad (3.62)$$

The analysis methods of damage showed that use of the ABS is the most suitable one and two-way damage followed crypto conversions, thus reducing the power of the alphabet while forming a cryptogram Mc IAMB Alice. Distance unity for the first method (expression 3.31) will be transformed:

$$U_0 = \frac{\sum_{i=1}^m \left(H(CHD^{(i)}) \right) + H(KU_i^{EC})}{B \log |I|}. \quad (3.63)$$

This system is based on a distortion of irreparable damage and sustainability through the use of encryption in the future based on the IAMB. This makes it impossible to know ciphertext unprofitable text.

Distance unity for the second method (expression 3.31) will be transformed:

$$U_0 = \frac{H(KU_i^{EC}) + H(FTC/FT_{CH}) + H(DCH/D_{CH})}{B \log |I|} + \frac{\sum_{i=1}^m (H(CHD^{(i)}) + H(KU_i^{EC}))}{B \log |I|}. \quad (3.64)$$

The second option can increase the distance by unity compared to the first method. Table 3.17 These results depending on the length of the input sequence algorithm MV2 on the number of CPU cycles to perform basic operations in program implementation.

Table 3.17. — Research results depending on the length of the input sequence algorithm MV2 on the number of CPU cycles

The length of the code sequence		MV2		
		10	100	1000
Number of function calls that implement basic operations	summation	3942	28673	275499
	difference	1794	3810	23881
	division	3274	4804	20104
	multiplication	19	109	1009
	comparison	8939	60963	578784
Sum		17968	98359	899277
The duration of the functions in milliseconds *	summation	19.53	93.58	2297.36
	difference	8.89	12.43	199.14
	division	16.22	15.68	167.65
	multiplication	0.09	0.36	8.41
	comparison	44.28	198.96	4826.43
Sum		89	321	7499
The duration of the functions in milliseconds *		89	321	7499

Note: * — the length of 1000 operations per processor cycle: reading character — 27 cycles, comparing lines — 54 cycles, string concatenation — 297 cycles; ** — taken for calculating processor clocked at 2GHz based operating system 5 %

Table 3.18 represents the results of research evaluation time and speed performance and application procedures for the removal of damage.

Table 3.18. — Research results and evaluation of temporary speed performance and application procedures for the removal of damage

Indexes	The length of the code sequence	Time (sec)	The capacity of the algorithm, Rate (bytes/sec)	Recycling processor cores (ticks)	Complexity of the algorithm, Per (cpb)
Number of function calls that implement basic operations	10	0.089	112.3596	90	0.801
	100	0.321	311.5265	322	1.034
	1000	7.499	133.3511	7500	66.166

Thus, the analysis of the basic principles of construction IAMB McEliece and systems for multichannel cryptography codes allows unprofitable to develop hybrid cryptosystem based on modified asymmetric crypto code of Mc Alice and multichannel cryptography systems for loss-making codes. A distinctive feature of «classical» approach of forming a hybrid cryptosystem is to use asymmetric crypto-code constructions (refer to secret evidence-based models of stability) with fast crypto conversions (rate of change comparable to the speed crypto conversions in BSC)

Consider practical algorithms of cryptogram and decrypt the proposed hybrid cryptosystem. Fig. 3.21, 3.22, 3.23 algorithms are forming cryptograms/codogram and decoding codogram a hybrid cryptosystem (respectively).

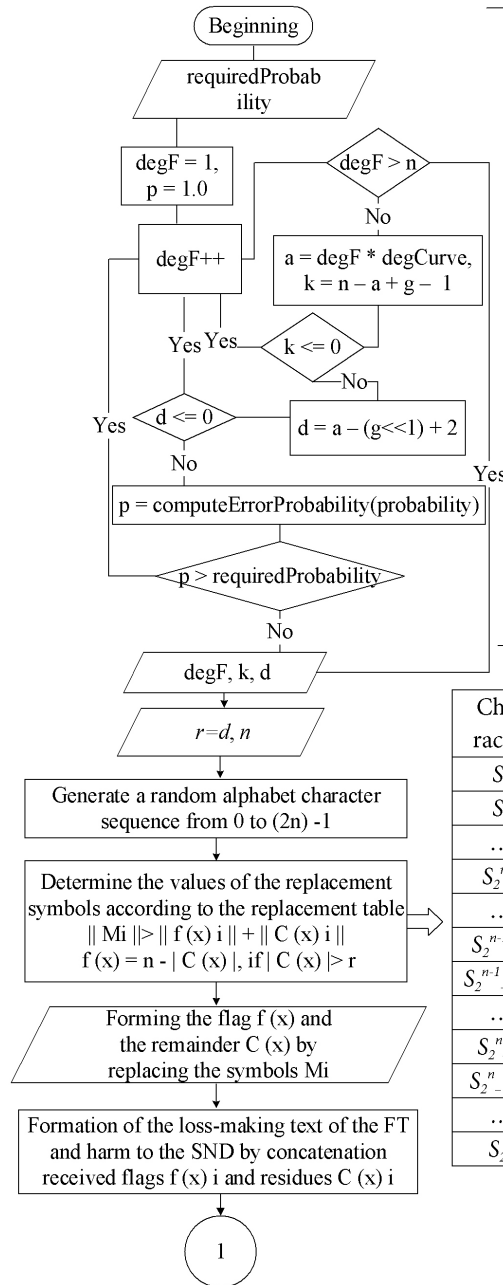
If the source code had some merit, for such a system is flawed text with complete enumeration of all the field of encryption keys and key losses are only meaningful text output level, provided that the length of cipher text more distance unity [9].

Algorithms allow hybrid cryptosystem when hiding unprofitable cipher-text SFT/CHFT all its possible values define additional key field:

$$U_0 = \frac{H(CFT / CH_{FT}) + \sum_{i=1}^m (H(CHD^{(i)})) + H(KU_i^{EC})}{B \log |I|}. \quad (3.65)$$

If additional loss concealment last cipher text SND/CHD because of its smallness and proportionality of the cipher text unprofitable text CFT/CHFT unity distance can be further increased:

$$U_0 = \frac{H(CHD / CH_D) + H(CFT / CH_{FT}) + \sum_{i=1}^m (H(CHD^{(i)})) + H(KU_i^{EC})}{B \log |I|}. \quad (3.66)$$



Stage 1. Setting the code parameters

requiredProbability - The probability of block distortion is given.

n - total number of characters in the code (code length),

k - number of information symbols, *d* is the minimum distance of Heming code combinations;

g - the genus of the curve, *degF* - degree of generator function, *degCurve* is the degree of curve.

Stage 2. Damage

Character	Remainder length	Remainder $C(x)$	Flag $f(x)$
S_1	r	0^r	$0^{n-r-1}1$
S_2	r	$0^{r-1}1$	$0^{n-r-1}1$
...	...	...	...
$S_{2^r+1}^r$	$r+1$	0^{r+1}	$0^{n-r-2}1$
...	...	...	...
$S_{2^{n-1}-2}^{n-1-r}$	$n-2$	1^{n-2}	01
$S_{2^{n-1}-2+1}^{n-1-r}$	$n-1$	0^{n-1}	1
...	...	...	...
$S_{2^n-2}^{n-r}$	$n-1$	1^{n-1}	1
$S_{2^n-2+1}^{n-r}$	r	0^r	0^{n-r}
...	...	...	...
$S_{2^n}^n$	r	1^r	0^{n-r}

$f(x)$ - flag,

$C(x)$ - the balance

Fig. 3.20. Codogram forming a hybrid crypto-code design

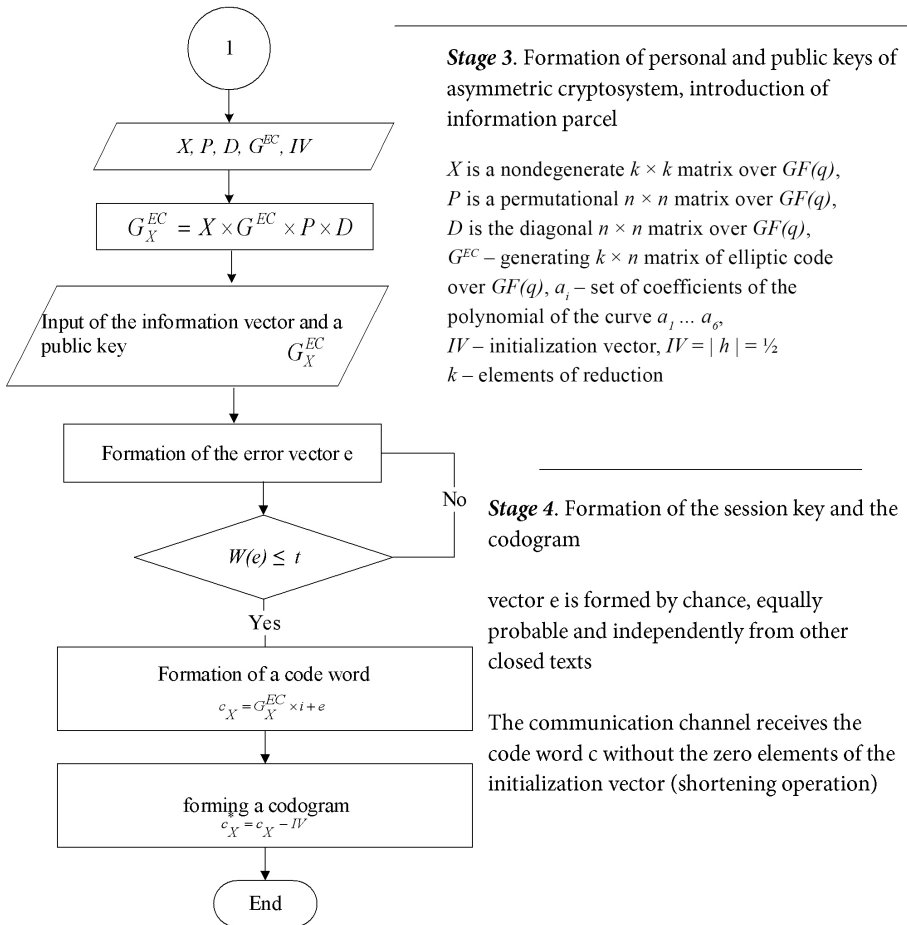
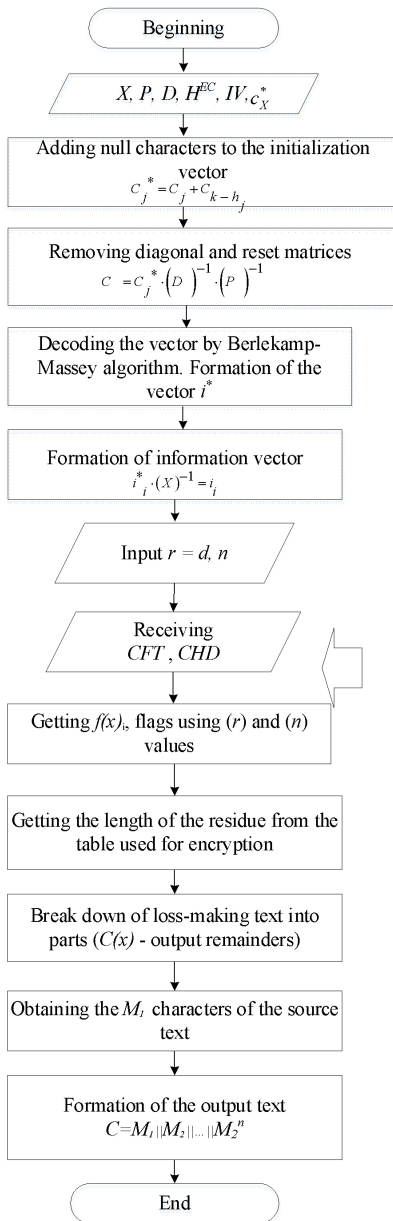


Fig. 3.21. Codogram forming a hybrid crypto-code design

Thus, multichannel cryptography based unprofitable codes allows integration of cryptographic systems, bringing together under one concept crypto-code design (MNCCS McEliece on MEC) system and to unprofitable codes that complement each other, will provide the required performance security and reliability and enrich the total system of its properties.

Consider a formal description of the proposed HCCDUC based NCCS McEliece and Niederreiter at MEC.



Stage 1. Setting the parameters of the code, entering a personal key and a codogram

X – a non-degenerate $k \times k$ Matrix over $GF(q)$,

P – the permutational $n \times n$ matrix over $GF(q)$,

D – the diagonal $n \times n$ matrix over $GF(q)$,

G^{EC} – singular $k \times n$ matrix of elliptic code over $GF(q)$, a_i

– set of the polynomial curve coefficients $a_1 \dots a_\phi$

IV – initialization vector, $IV = |h| = \frac{1}{2}$

k – elements of reduction

Stage 2. Decoding the codogram

Character	Remainder length	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}	$0 1$
$M_{2^{n-1}-2+1}^r$	$n-1$	0^{n-1}	1
...	...	...	...
$M_{2^{n-2}}^r$	$n-1$	1^{n-1}	1
$M_{2^{n-2}+1}^r$	r	0^r	0^{n-r}
...	...	...	...
$M_{2^n}^n$	r	1^r	0^{n-r}

Stage 3. Restoring the message to the damaged item

$f(x)$ – flag,

$C(x)$ – remainder

Fig. 3.22. Codogram decoding a hybrid crypto-code design

3.2.2 The development of mathematical models of hybrid crypto-code constructions based on asymmetric crypto-modified code of McEliece and Niederreiter on modified geometrical codes

Consider a formal description of the modified crypto-code system to McEliece unprofitable codes used in two factors authentication protocol.

To build mathematical models use the main provisions of [46] for a formal mathematical definition of classified systems. In work [7] the formal description of mathematical model MNCCS McEliece on modified elliptical codes in [9] the universal mechanism of injury and modes of transmission systems for loss-making codes.

Mathematical model HCCDUC McEliece-based shortening (reduction information symbols) formally given the totality of these elements [7]:

- the set of open-source: $M = \{M_1, M_2, \dots, M_{q^k}\}$, where $M_i = \{I_0, I_{h_1}, \dots, I_{h_j}, I_{k-1}\}$, $\forall I_j \in GF(q)$, h_j — information symbols are zero, |set closed texts (codogram) — $C = \{C_1, C_2, \dots, C_{q^k}\}$, where $C_i = (c_{x_0}^*, c_{h_1}^*, \dots, c_{h_j}^*, c_{x_{n-1}}^*) \quad \forall c_{x_j}^* \in GF(q)$

- set direct mappings (based on the use of public key — generative matrix): $\phi = \{\phi_1, \phi_2, \dots, \phi_s\}$, where $\phi_i : M \rightarrow C_{h_i} \quad i = 1, 2, \dots, s$;

- set of inverse mapping (through the use of closed (private) key — masking matrix): $\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, \dots, \phi_s^{-1}\}$, where $\phi_i^{-1} : C_{h_i} \rightarrow M \quad i = 1, 2, \dots, s$;

- a set of keys that parameterize direct reflection (public key authorized user): $K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, \dots, K_{s_{a_i}}\} = \{G_X^{EC_1}, G_X^{EC_2}, \dots, G_X^{EC_s}\}$, where $G_X^{EC_i}$ — generative $k \times n$ matrix disguised random code block geometrical (n, k, d) with elements of the code $GF(q)$ i.e. $\phi_i : M \xrightarrow{K_{ia_i}} C_{h_i} \quad i = 1, 2, \dots, s$ a_i — a set of polynomial curve coefficients $a_1 \dots a_6$, $\forall a_i \in GF(q)$ clearly poses a specific set point curve space P^2 .

- set texts unprofitable CFT, $CFT = \{CFT_1, CFT_2, \dots, CFT_{q^k}\}$;

- set loss CHD, $CHD = \{CHD_1, CHD_2, \dots, CHD_{q^k}\}$;

- set of direct damage (on the basis of key -KiMV2 And algorithm MV2) — $E = \{E^1_{K_{MV2}}, E^1_{K_{MV2}}, \dots, \phi^S_{K_{MV2}}\}$, $i = 1, 2, \dots, s$, $f(x)_i$ — flag (loss, CHD), $C(x)_i$ — balance (unprofitable text SFT); $f(x) = n - |C(x)|$, if $|C(x)| > r$, where r — a parameter $r \in_R Z_{q^m}$, $0 < r < n$;

- set mappings MV2 F_n^r given bijective mapping between multiple permutations $\{S_1, S_2, \dots, S_{2^n}\}$ and set $\#F_n^r, \#F_n^r = \#\{(c, f)\} = 2^n!$;

- set meaningful text (on the basis of key -*KiMV2* And algorithm *MV2*):

$$E^{-1} = \{E_{K_{MV2}}^{-1}, E_{K_{MV2}}^2, \dots, E_{K_{MV2}}^S\},$$

where $E_{K_{MV2}}^{-1} : \|f(x)_i\| + \|C(x)_i\| \rightarrow M, i = 1, 2, \dots, s, f(x)_i$ — flag (loss, CHD), $C(x)_i$ — balance (unprofitable text SFT); $f(x) = n - |C(x)|$, if $|C(x)| > r$, where r — a parameter: $r \in_R Z_{q^m}$;

- a set of keys that parameterize reverse mapping (private (secret) key authorized user):

$$K^* = \{K_1^*, K_2^*, \dots, K_s^*\} = \{\{X, P, D\}_1, \{X, P, D\}_2, \dots, \{X, P, D\}_s\} \quad \{X, P, D\}_i = \{X^i, P^i, D^i\},$$

where X^i — masking nondegenerate randomly generated equally probable source keys $k \times k$ matrix elements of $GF(q)$; P^i — rearrangement randomly generated equally probable source keys $n \times n$ matrix elements of $GF(q)$; D^i — diagonal matrix formed from a source key elements of $GF(q)$ that is $\phi_i^{-1} : C \xrightarrow{K_i^*} M, i = 1, 2, \dots, s$ the complexity of reverse mapping ϕ_i^{-1} without knowledge of the key $K_i^* \in K^*$ related to the decision-theoretic challenger decoding the random code (code common position).

- a set of keys transform unprofitable codes $K_{MV2}^i \in K_{MV2}^i$.

Initial data considered in describing the asymmetric crypto-code information protection system are:

- geometrical block (n, k, d) code C_{k-h_j} over $GF(q)$, ie the set of code words $C_i \in C_{k-h_j}$ such that the equality $C_i H^T = 0$, where H — test matrix geometrical block code;

- a_i — a set of polynomial curve coefficients $a_1 \dots a_6, \forall a_i \in GF(q)$ clearly poses a specific set point curve P^2 space to form a matrix that generates;

- h_j — information symbols are zero, $|h| = 1/2k$, i.e. $I_i = 0, \forall I_i \in h$;

- masking matrix display given set of matrices $\{X, P, D\}_i$, where X — non-degenerate $k \times k$ matrix over $GF(q)$, P — rearrangement $n \times n$ matrix over $GF(q)$ with a non-zero element in each row and each column of the matrix, D — diagonal $n \times n$ matrix over $GF(q)$ with nonzero elements on the main diagonal;

- r — a parameter $r \in_R Z_{q^m}, Z_{q^m} = \{0, 1 \dots 2^n - 1\}$;

- n — a parameter $n \in_R Z_{q^m}, Z_{q^m} = \{0, 1 \dots 2^n\}$;

- set mappings *MV2* F_n^r .

In MNCCS McEliece modified (shortened) geometrical (n, k, d) code C_{k-h_j} with fast decoding algorithm disguised as random (n, k, d) code $C_{k-h_j}^*$ by

multiplying generative matrix of code GES C_{k-h_j} for masking matrix that are in secret X^u , P^u and D^u [7] to form the public key of the authorized user:

$$G_X^{ECu} = X^u \cdot G^{EC} \cdot P^u \cdot D^u, u \in \{1, 2, \dots, s\}, \quad (3.67)$$

where G^{EC} — generative $n \times k$ geometrical block matrix (n, k, d) with elements of the code $GF(q)$ is based on the use of user-selected polynomial curve coefficients $a_1 \dots a_6$, $\forall a_i \in GF(q)$ clearly that define a specific set point curve space P^2 .

Forming a closed text $C_j \in C_{h_r}$ introduced by the plaintext $M_i \in M$ and given public key G_X^{ECu} , $u \in \{1, 2, \dots, s\}$ carried out by forming a codeword masked with adding code to it randomly generated vector $e = (e_0, e_1, \dots, e_{n-1})$ $C_j = \phi_u(M_i, G_X^u) = M_i \cdot (G_X^u)^T + e$. Hemet and weight (the number of non-zero elements) vector does not exceed the capacity used algebraic correcting code block: $0 \leq w(e) \leq t = \left\lfloor \frac{d-1}{2} \right\rfloor$, $[x]$ — the whole of real numbers.

For each closed text which formed $C_j \in C_{h_r}$ corresponding vector $e = (e_0, e_1, \dots, e_{n-1})$ acts as a one-time session key that is specific to E_j vector e formed by accident, equally probable and closed independently of the other texts.

In the algorithm MV2 fed:

$$C_j^* = C_j - C_{k-h_j}, E_{K_{MV2}} : C_j^* \rightarrow \|f(x)_i\| + \|C(x)_i\|. \quad (3.68)$$

In the channel $\|f(x)_i\|$ and $\|C(x)_i\|$ this transfer can be carried out by one or two independent channels.

On the receiving side the authorized user who knows the rules of harm F_n^r , masking, number and location information null characters can use speed decoding algorithm geometrical code (polynomial complexity) to recover the plaintext:

$$E_{K_{MV2}} : \|f(x)_i\| + \|C(x)_i\| \rightarrow C_j^*, M_i = \phi_u^{-1}(C_j^*, \{X, P, D\}_u). \quad (3.69)$$

To restore the plaintext authorized user adds zero information symbols $C_j^* = C_{h_r} + C_{k-h_j}$ recovered from a closed text C_j takes action secret permutation and diagonal matrices P^u and D^u :

$$\begin{aligned} C &= C_j^* \cdot (D^u)^{-1} \cdot (P^u)^{-1} = (M_i \cdot (G_X^u)^T + e) \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \\ &= (M_i \cdot (X^u \cdot G \cdot P^u \cdot D^u)^T + e) \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \\ &= M_i \cdot (X^u)^T \cdot (G)^T \cdot (P^u)^T \cdot (D^u)^T \cdot (D^u)^{-1} \cdot (P^u)^{-1} + e \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \\ &= M_i \cdot (X^u)^T \cdot (G)^T + e \cdot (D^u)^{-1} \cdot (P^u)^{-1}. \end{aligned} \quad (3.70)$$

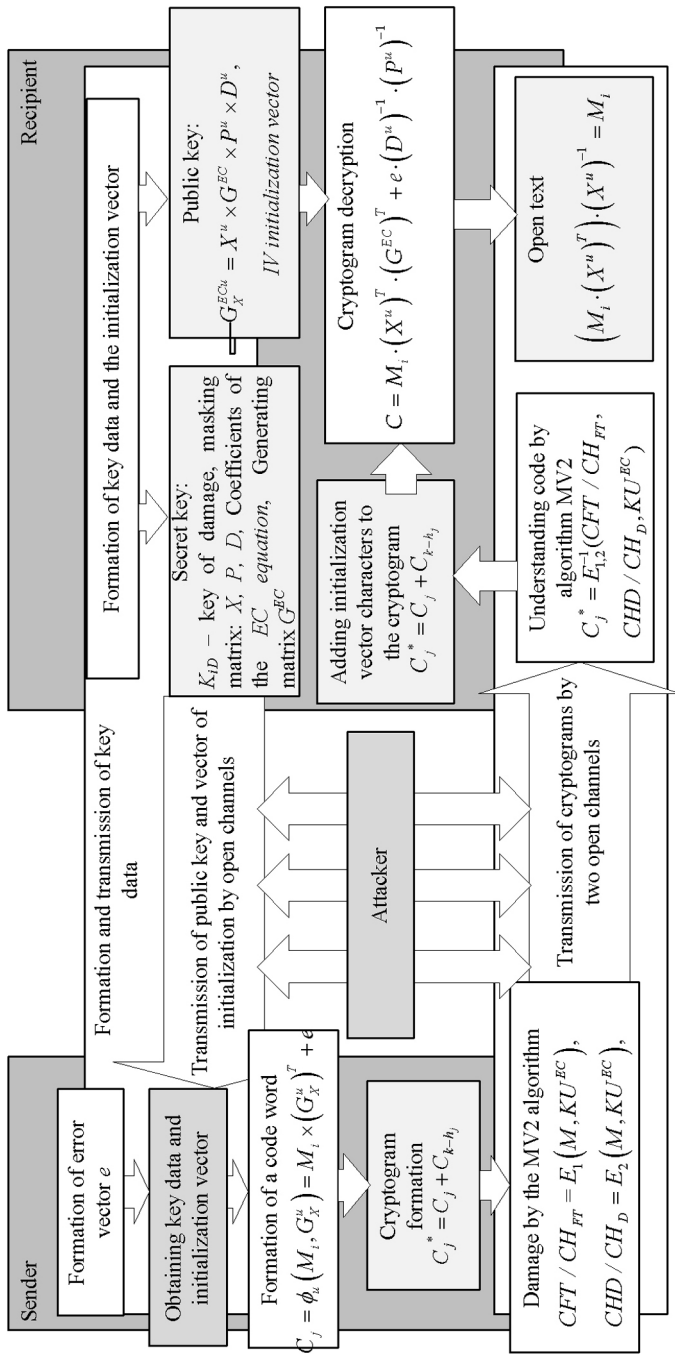


Fig. 3.23. Communications protocol SI in ABS using HCCDUC on MNCCS McEliece MEA on the truncated second method for damage

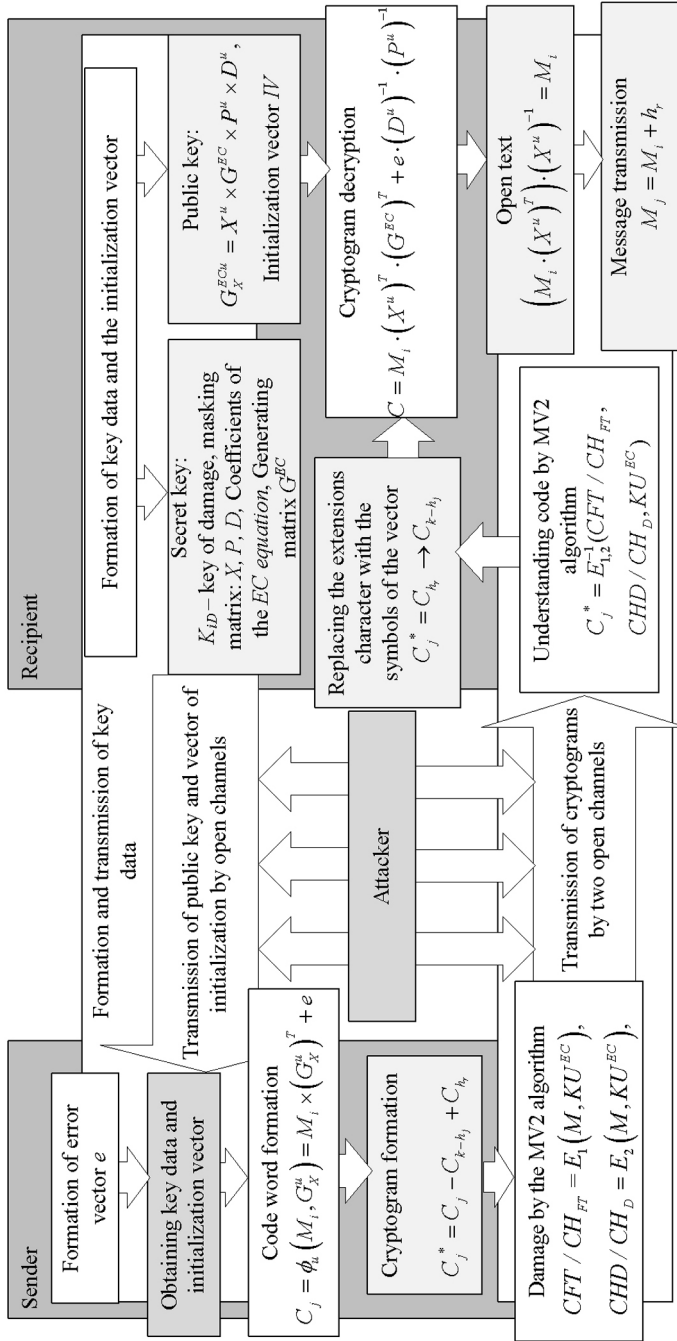


Fig. 3.24. Communications protocol SI in ABS using HCCDUC on MNCCS McEliece MEA on the truncated second method for damage

Decode received vector algorithm Berlekempa-Messi [34, 35, 36]:

$$C = M_i \cdot (X^u)^T \cdot (G^{EC})^T + e \cdot (D^u)^{-1} \cdot (P^u)^{-1}. \quad (3.71)$$

That gets rid of the second term and the multiplier $(G)^{EC^T}$ in the first term on the right side of equality, then remove the masking effect of the matrix X^u . For the result of decoding $M_i^* \cdot (X^u)^T$ be multiplied by $(X^u)^{-1}$:

$$(M_i \cdot (X^u)^T) \cdot (X^u)^{-1} = M_i.$$

The resulting solution — are plain text M_i .

Block diagram of protocol information in real time using MNCCS McEliece with modified (shorter) elliptical codes shown in Fig. 3.23, with modified extended in Fig. 3.24.

The main difference is the use of extended codes provisions symbols reduction in MNCCS Mc Alice, with their subsequent replacement with information symbols open SI.

In ext. as examples of protocols SI in ABS based on HCCDUC months (shortened/lengthened) based MNCCS McEliece, listing software model proposed HCCDUC for MEC is provided in the add.D.

Consider a formal description of mathematical models of hybrid CCD Niederreiter that given the totality of these elements [9]:

the set of open-source $M = \{M_1, M_2, \dots, M_{q^k}\}$, where $M_i = \{e_0, e_{h_1}, \dots, e_{h_k}, e_{e-1}\}$,

$\forall e_e \in GF(q)$, h_e — symbols vector error is zero, $|h| = \frac{1}{2}k$, $e_i = 0$, $\forall e_i \in h$;

– set closed texts $S = \{S_0, S_1, \dots, S_{q^r}\}$, where $S_i = \{S_{X_0}^*, S_{h_1}^*, \dots, S_{h_j}^*, S_{X_r}^*\}$,

$\forall S_{X_r} \in GF(q)$;

– set direct mappings (based on the use of public key — with the elliptical matrix code (EC): $\varphi = \{\varphi_1, \varphi_2, \dots, \varphi_r\}$, where $\varphi_i : M \rightarrow S_{r-h_e}, i = 1, 2, \dots, e$;

– set of inverse mapping (through the use of closed (private) key — masking matrix) $\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \dots, \varphi_r^{-1}\}$, where $\varphi_i^{-1} : S_{r-h_e} \rightarrow M, i = 1, 2, \dots, e$;

– a set of keys that parameterize direct reflection (public key authorized user):

$$KU_{a_i} = \{KU_{1_{a_i}}, KU_{2_{a_i}}, \dots, KU_{r_{a_i}}\} = \{H_{X_{a_i}}^{EC_1}, H_{X_{a_i}}^{EC_2}, \dots, H_{X_{a_i}}^{EC_r}\}, \quad (3.72)$$

where $H_{X_{a_i}}^{EC_i}$ — verification $r \times n$ matrix disguised random code block geometrical (n, k, d) code with elements $GF(q)$, i.e. $\varphi_i : M \xrightarrow{KU_{1_{a_i}}} S_{r-h_e}^*, i = 1, 2, \dots, e$;

- a_i — a set of polynomial curve coefficients $a_1 \dots a_o, \forall a_i \in GF(q)$ specifies a specific set point curve space P^2 ;
- a set of keys that parameterize reverse mapping (private (secret) key authorized user):

$$KR = \{KR_1, KR_2, \dots, KR_r\} = \left\{ \begin{aligned} &\{X, P, D\}_1, \\ &\{X, P, D\}_2, \dots, \{X, P, D\}_r \end{aligned} \right\},$$

$$\{X, P, D\}_i = \{X^i, P^i, D^i\}, \quad (3.73)$$

where X^i — masking nondegenerate randomly generated equally probable source keys $k \times k$ matrix elements of $GF(q)$; P^i — rearrangement randomly generated equally probable source keys $n \times n$ matrix elements of $GF(q)$; D^i — diagonal matrix formed from a source key elements of $GF(q)$; that is $\phi_i^{-1} : S_{r-h_e}^* \xrightarrow{KR_i} M, i = 1, 2, \dots, s$, the complexity of reverse mapping ϕ_i^{-1} without knowledge of the key $K_i^* \in K^*$ related to the decision-theoretic challenger decoding the random code (code common position);

- set texts unprofitable $CFT, CFT = \{CFT_1, CFT_2, \dots, CFT_{q^k}\}$;
- set loss $CHD, CHD = \{CHD_1, CHD_2, \dots, CHD_{q^k}\}$;
- set of direct damage (on the basis of key – K_{iMV2} And algorithm MV2): $E = \{E_{K_{MV2}}^1, E_{K_{MV2}}^2, \dots, E_{K_{MV2}}^S\}, i = 1, 2, \dots, s; f(x)_i$ — flag (loss, CHD), $C(x)_i$ — balance (unprofitable text CFT); $f(x) = n - |C(x)|$, if $|C(x)| > r$, where r — a parameter $r \in_R Z_{q^m}, 0 < r < n$;
- set mappings MV2 F_n^r given bijective mapping between multiple permutations $\{S_1, S_2, \dots, S_{2^n}\}$ and set $\#F_n^r, \#F_n^r = \#\{(c, f)\} = 2^n!$;
- set meaningful text (on the basis of key – K_{iMV2} and algorithm MV2): $E^{-1} = \{E_{K_{MV2}}^{1^{-1}}, E_{K_{MV2}}^{2^{-1}}, \dots, E_{K_{MV2}}^{S^{-1}}\},$ where $E_{K_{MV2}}^{-1} : \|f(x)_i\| + \|C(x)_i\| \rightarrow M, i = 1, 2, \dots, s; f(x)_i$ — flag (loss, CHD), $C(x)_i$ — balance (unprofitable text CFT); $f(x) = n - |C(x)|$, if $|C(x)| > r$, where r — a parameter $r \in_R Z_{q^m}$.

Initial data considered in describing the asymmetric crypto-code information protection system are:

- equilibrium code over $GF(q)$, i. e. the set of sequences of length n and weight $w(\epsilon_i)$;
- geometrical block (n, k, d) code C over $GF(q)$, i. e. the set of code words $C_i \in C$ such that the equality $C_i H^T = 0$, where H — test matrix geometrical block code;

- IV —initialization vector, $IV = |h| = 1/2$ Do not — elements of reduction
- $(h_e$ — Symbols vector error is zero, $|h| = 1/2$ i. e. $e_i = 0, \forall e_i \in h$);
- masking matrix display given set of matrices $\{X, P, D\}_i$, where X — non-degenerate $k \times k$ matrix over $GF(q)$, P — rearrangement $n \times n$ matrix over $GF(q)$ with a non-zero element in each row and each column of the matrix, D — diagonal $n \times n$ matrix over $GF(q)$ with nonzero elements on the main diagonal;
- r — a parameter $r \in_R Z_{q^m}, Z_{q^m} = \{0, 1, \dots, 2^n - 1\}$,
- n — a parameter $n \in_R Z_{q^n}, Z_{q^n} = \{1, \dots, 2^n\}$;
- set mappings $MV2 = F_n^r$.

Based coding equilibrium is formed into closed $C_j \in C$ introduced by the plaintext $M_i \in M$ and given key H_X^{ECu} , $u \in \{1, 2, \dots, s\}$ carried out by forming syndrome (in terms of noise immunity encoding) sequence S_{X_i} corresponding equilibrium sequence $M_i = e = \{e_0, e_1, \dots, e_{n-1}\}$:

$$S_{X_i} = \phi_u(M_i, H_X^{ECu}) = M_i \times (H_X^{ECu})^T.$$

Hemet and weight (the number of non-zero elements) vector does not exceed the capacity used algebraic correcting block (n, k, d) CODE:

$$\forall i: 0 \leq w(M_i) \leq t = \left\lfloor \frac{d-1}{2} \right\rfloor. \quad (3.74)$$

Power sets M and C defined acceptable range of weights $w(M_i)$ in general (for all permissible values $w(M_i)$) are:

$$m = \sum_{i=0}^t (q-1)^i \times C_n^i, \quad (3.75)$$

where C_n^i — binomial coefficient $C_n^i = \frac{n!}{i! \cdot (n-i)!}$.

The most appropriate size $w(M_i)$ choose a value to the required safety data SI in ABS.

Then, for $w(M_i) = \text{const} = w(e)$ we have: $m = (q-1)^{w(e)} \times C_n^{w(e)}$ and sequence $M_i = \{e_0, e_1, \dots, e_{n-1}\}$ to set $M = \{M_1, M_2, \dots, M_m\}$ formed as a result of some reflection ψ , implemented by the excess coding nedviykovyy equilibrium codes nonredundant information sequences.

Formed into closed $C_j \in C$ uniquely corresponds vector $M_i = \{e_0, e_1, \dots, e_{n-1}\}$.

Create the initialization vector $IV = EC - h_j$, h_j — information symbols are zero, $|h| = 1/2k$, i.e. $I_i = 0, \forall I_i \in h$.

Forming truncated error vector $ex = e(A) - IV$.

The public key is formed by multiplying matrix geometrical checking code to disguise matrix: $H_X^{ECu} = X^u \cdot H \cdot P^u \cdot D^u$, $u \in \{1, 2, \dots, s\}$, where H^{EC} — testing $n \times (n - k)$ geometrical block matrix (n, k, d) with elements of the code $GF(q)$.

In MV2 algorithm goes syndrome sequence: $S_{r-h_e}^* = (e_n - h_e) \times H_X^{ECT}$.

In MV2 sequence $S_{r-h_e}^*$ balance and becomes a flag:

$$E_{K_{MV2}} : S_{r-h_e}^* \rightarrow \|f(x)_i\| + \|C(x)_i\|. \quad (3.76)$$

In the channel coming $\|f(x)_i\|$ and $\|C(x)_i\|$, this transfer can be carried out by one or two independent channels.

On the receiving side the authorized user who knows the rules of harm F_n' masking (sets of matrices $\{X, P, D\}_u = \{X^u, P^u, D^u\}$) and initialization vector (number of characters and places zero vector error):

$$E_{K_{MV2}}^{-1} : \|f(x)_i\| + \|C(x)_i\| \rightarrow S_{r-h_e}^*, \quad (3.77)$$

Generates code sequence as one (any) of the possible solutions to the equation:

$$S_{r-h_e}^* = A_{X_i}^* \cdot H_{X_j}^T \quad (3.78)$$

That is a vector $A_{X_i}^*$ which expanded the amount of: $A_{X_i}^* = A_{X_i} + M_i$, where A_{X_i} — one (any) of your code disguised code words of checking matrix $H_{X_j}^T$ that is $A_{X_i} \times H_{X_j}^T = 0$.

Further, the authorized user using a set of matrices $\{X, P, D\}_u = \{X^u, P^u, D^u\}$ vector forms: $\bar{A}^* = A_X^* \cdot (D^u)^{-1} \cdot (P^u)^{-1}$ ie code sequence $A_{X_i}^*$.

After substitution, we get the equality:

$$\begin{aligned} \bar{A}^* &= A_X^* \cdot (D^u)^{-1} \cdot (P^u)^{-1} = (A_{X_i} + M_i) \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \\ &= A_{X_i} \cdot (D^u)^{-1} \cdot (P^u)^{-1} + M_i \cdot (D^u)^{-1} \cdot (P^u)^{-1}. \end{aligned} \quad (3.79)$$

The delegate, who formed vector has the ability to use fast (polynomial complexity) algorithm for decoding noise immunity and thus form a vector:

$$\bar{A}^* = A_X^* \cdot (D^u)^{-1} \cdot (P^u)^{-1} \text{ and vector } M_i^u = M_i \cdot (D^u)^{-1} \cdot (P^u)^{-1} \quad (3.80)$$

To restore equilibrium sequence information M_i vector multiply enough again M_i^u masking the matrix D^u and P^u . But the second order:

$$M_i = M_i^u \cdot P^u \cdot D^u = M_i \cdot (D^u)^{-1} \cdot (P^u)^{-1} \cdot P^u \cdot D^u = M_i \quad (3.81)$$

Formation of the desired error vector e : $M = M_i + IV$.

Analysis of the practical implementation of algorithms for encryption/decryption in HCCDUC Niederreiter shows that the formation of cryptograms (syndrome) after the formation of the error vector encoding algorithm based on equilibrium initialization vector (formed under VFR [8] trusted in the center and closed channels transmitted via the ABS issuer and acquirer banks or vector MV2 algorithm is encrypted and transmitted to two independent channels open) produced reductions — h_e (vector characters bugs, zero) $|h| = 1/2e$, i.e. $e_i = 0, \forall e_i \in h$.

When deciphering cryptograms (after vector error before using the coding algorithm equilibrium) for information input "zero" symbols shortening. Algorithms for encryption and decryption are presented in Fig. 3.25–3.26, 3.27–3.28, respectively.

The algorithm forming a cryptogram IAMB Niederreiter represented as a sequence of the following steps:

Step 1. Putting information to be coding. Introduction to Public Key H_X^{EC} .

Step 2. Formation of the error vector e , whose weight does not exceed $\leq t$ — correcting ability elliptic code based coding algorithm nedviykovyy equilibrium [10, 18].

Step 3. Forming truncated error vector: $e_x = e(A) - IV$.

Step 4. Formation codogram: $S_{r-h_e}^* = (e_n - h_e) \times H_X^{ECT}$.

Step 5. Formation of unprofitable text (balance) and flag (loss):

$$E_{K_{MV2}} : S_{r-h_e}^* \rightarrow \|f(x)_i\| + \|C(x)_i\|.$$

Decoding algorithm in codogram IAMB Niederreiter represented as a sequence of the following steps:

Step 1. Obtaining meaningful text codogram based algorithm MV2:

$$E_{K_{MV2}}^{-1} : \|f(x)_i\| + \|C(x)_i\| \rightarrow S_{r-h_e}^*.$$

Step 2. Introduction codogram SX, which decode. Entering the private key — matrix X, P, D .

Step 3. Being one of the possible solutions to the equation:

$$S_{r-h_e}^* = \bar{A}^* \times (H_X^{EC})^T. \quad (3.82)$$

Step 4. Removing the diagonal action and commuting matrices:

$$\bar{A}^* = A_X^* \cdot D^{-1} \cdot P^{-1}. \quad (3.83)$$

Step 5. Decoding vector $\bar{A}$. Formation vector e_x' .

Step 6. Convert vector e_x' :

$$eh \, eh' = ' \times P \times D. \quad (3.84)$$

Step 7. Formation of the desired vector errors are:

$$e = e_x + IV. \quad (3.85)$$

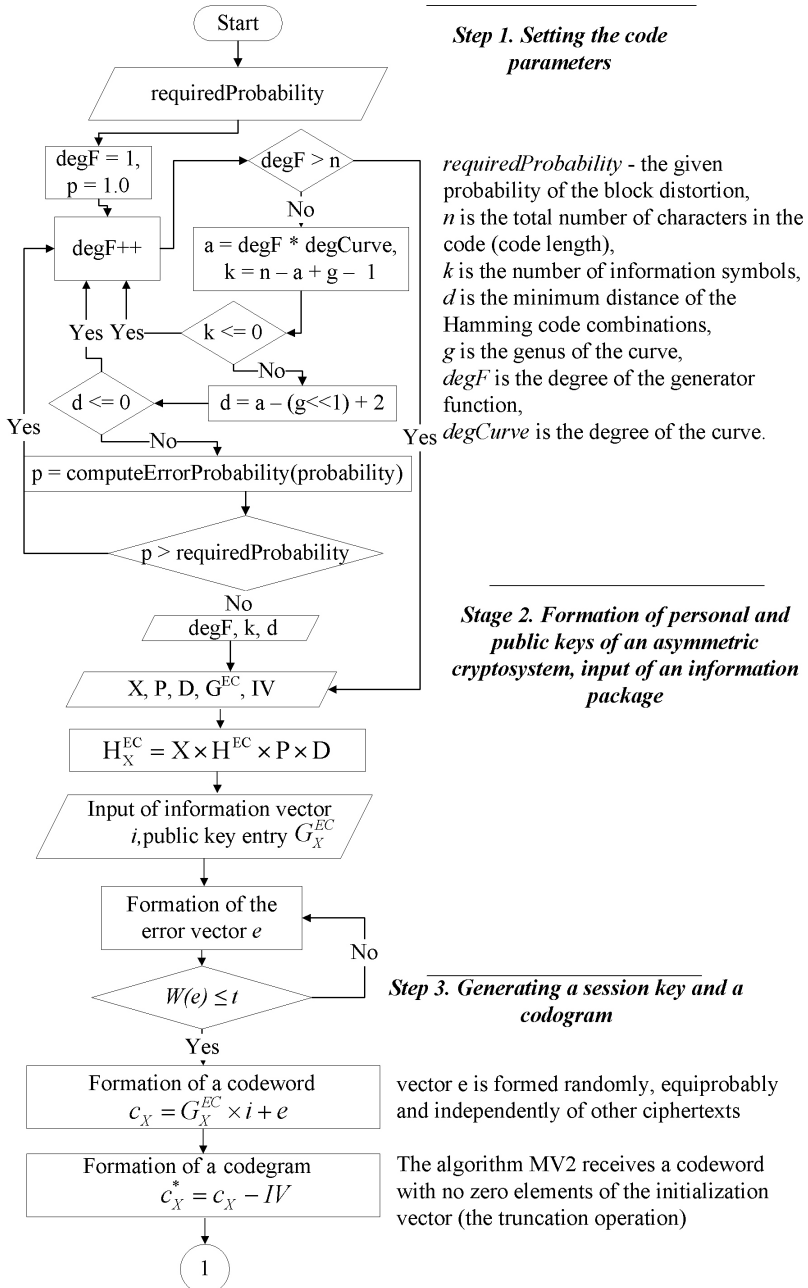


Fig. 3.25. Formation codogram in MCCDUC Niederreiter at MEC

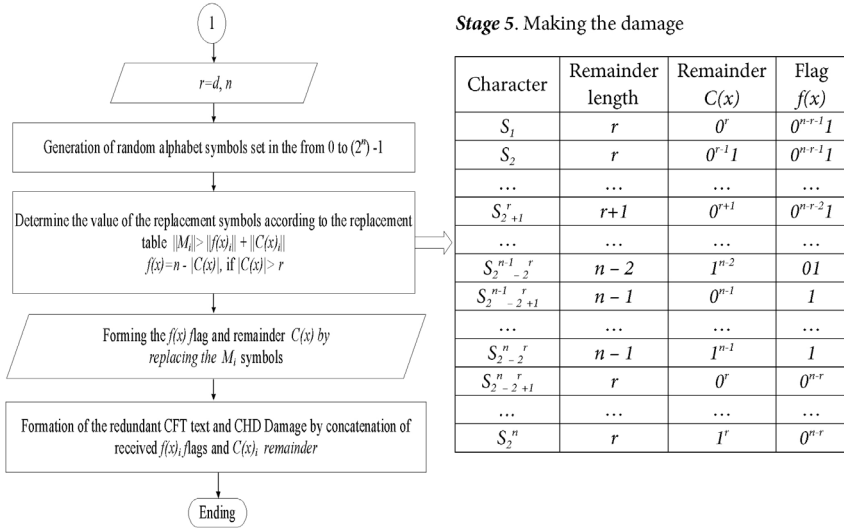


Fig. 3.26. Formation codogram in MCCDUC Niederreiter at MEC

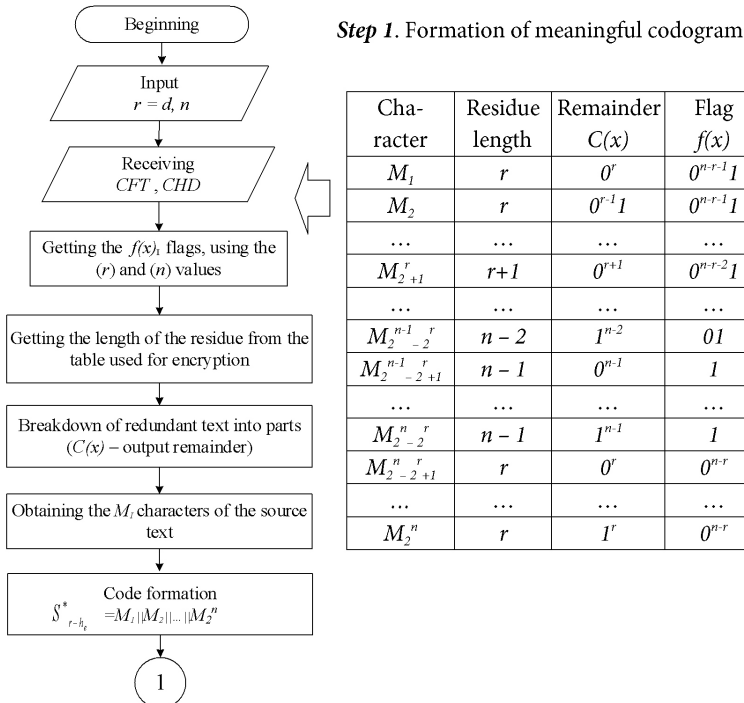


Fig. 3.27. Decoding codogram in MCCDUC Niederreiter at MEC

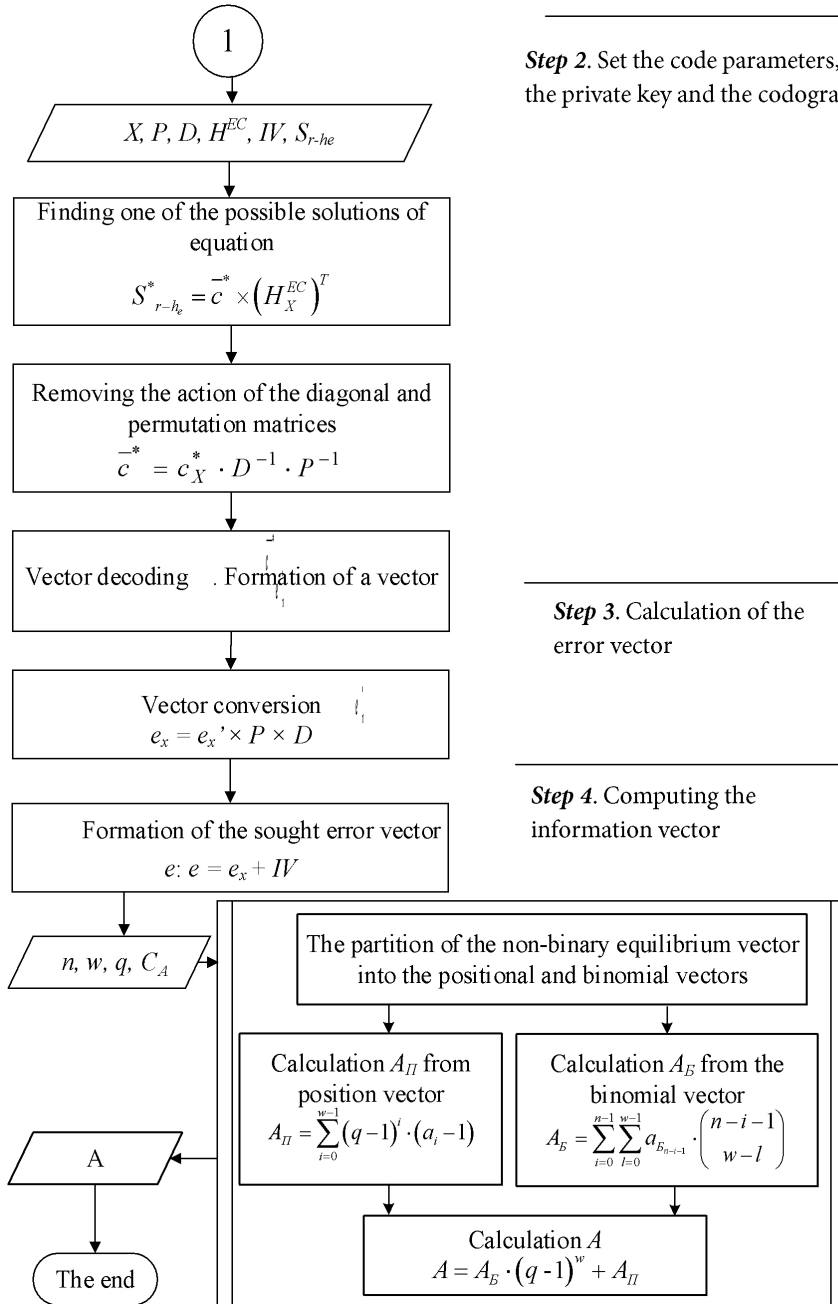


Fig. 3.28. Decoding codogram in MCCDUC Niederreiter at MEC

Step 8. Convert vector e on the basis of equilibrium code sequence information.

Consider the features offered HCCDUC McEliece for MES, a comparative evaluation of the basic properties (cryptoconversions speed, complexity break and so on).

3.2.3 Studying the properties of hybrid crypto-code designs on unprofitable codes

A comparative evaluation parameters MNCCS McEliece to MEA with HCCDUC using a modified elliptical codes. We introduce the following notation:

l_i — the length of the sequence information (block), which is the input of the CCS scheme (in bits); l_k — public key length (in bits); l_{k+} — private key length (in bits); l_s — codogram length (in bits); O_k — forming codogram complexity (number of group operations); O_{sk} — complexity decoding codogram (number of group operations); O_{k+} — the complexity of solving the problem analysis (the number of group operations); K_c — compression ratio balance; K_f — compression ratio of the flag; s — number of unprofitable segments of the text; $u(n)$, $v(r)$ — a positive number key loss; $z(m)$ — Rounds loss; L_0 — the length of the original text; L_{DT} — long unprofitable text.

For charting used conventional reduction (console): ukh/udh — Hybrid CCDUC with short MES/CCDUC hybrid with extended MES; uk — MNCCS with short MEAs; ud — MNCCS with a long month.

In calculating parameters cryptosystems used Galois field: for MNCCS with short/extended MEC — $GF(2^6)$, for hybrid CCDUC — $GF(2^4)$.

The length of sequence information (In bits) that the input of the TSP cryptosystem defined by the following expression: for HCCDUC to shortened codes:

$$l_i = l_z^c + l_z^f,$$

where: $l_z^c = K_c \times L + \frac{1}{K_f} \times s$ — length unprofitable text; $l_z^f = L + u \times s$ — length

loss; $s = \left\lceil \frac{L_0 - L_{DT}}{L_{DT}} \right\rceil$ — the number of unprofitable segments of text

$K_c = 1 - K_f \approx 0.758$ — compression ratio balance (unprofitable text) (When

$u=8$, $v=3$, $z=5$); $K_f = \frac{2 - 2^{v-u+1}}{u} \approx 0.242$ — compression ratio flag (loss)

(When $u=8$, $v=3$, $z=5$); $z = \frac{\log(u \times L) - 7}{\log(1/K_c)}$ — required for randomization

algorithm MV2, the number of permissible rounds of transformation. For HCCDUC extended to MEC: $l_t = 1 / 2k \times m + l_z^c + l_z^f$.

Table 3.19 in Fig. 3.38 The results of research difficulty forming cryptograms in different $GF(2^m)$.

Table 3.19.— Dependence difficulty forming cryptograms in different $GF(2^m)$

$GF(2^m)$	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

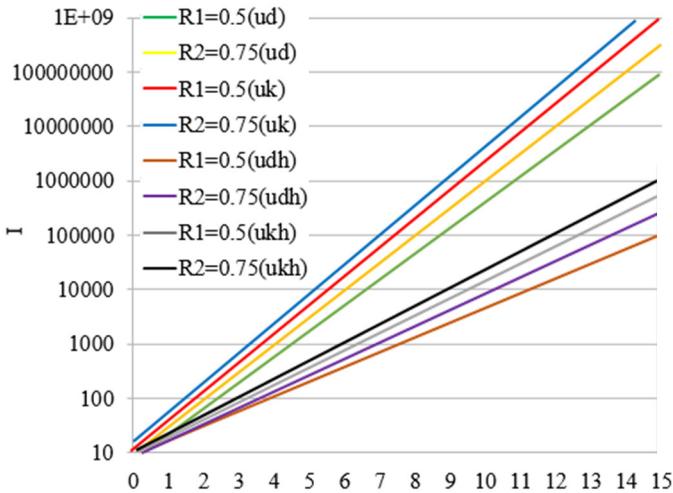


Fig. 3.29. Dependence difficulty forming cryptograms in different $GF(2^m)$

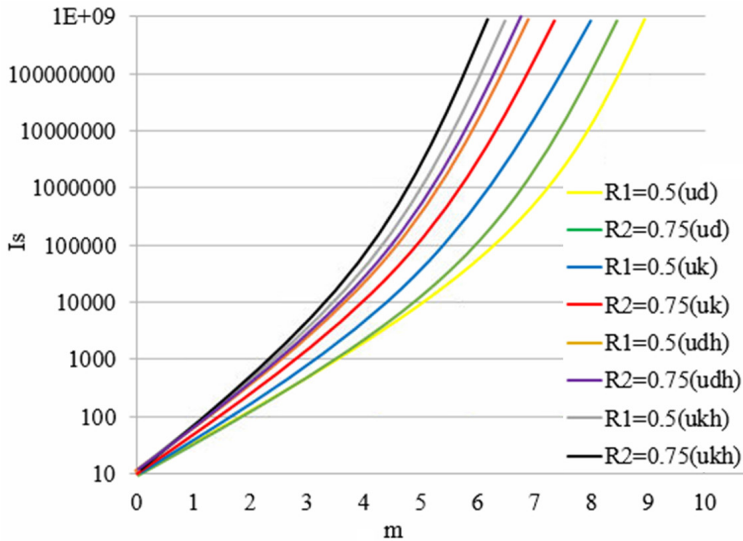
Length codogram (In bits) is determined by the expressions:

- for HCCDUC truncated at MEC: $l_s = (2\sqrt{q} + q + 1 - 1/2k) \times m$;
- HCCDUC extended for at MEC: $l_s = (2\sqrt{q} + q + 1 - 1/2k + 1/2k) \times m$.

Table 3.20 in Fig. 3.30 these results cryptogram decoding complexity in different $GF(2^m)$.

Table 3.20. — The research results cryptogram decoding complexity in different $GF(2^m)$

$GF(2^m)$	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. 3.30. Dependence difficulty decoding cryptograms in different $GF(2^m)$

Analysis of Table 3.19, 3.20, Fig. 3.29, 3.30 showed that the use of loss-making codes and further reduce power Galois field leads to a significant reduction of the complexity of the formation (≈ 12 times) and decoding (≈ 20 times) cryptograms.

The length of the public key (In bits) is the sum of the matrix elements G_X^{EC} and is given by the expressions:

- for HCCDUC truncated at MEC: $l_K = 1/2k \times (2\sqrt{q} + q + 1 - 1/2k) \times m$;
- HCCDUC extended for at MEC: $l_K = 1/2k \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k) \times m$.

The length of the secret key (In bits) is the sum of matrix elements X, P, D (in bits) and given expressions for HCCDUC to shortened codes:

$$l_{K_+} = 1/2k \left\lceil \log_2 (2\sqrt{q} + q + 1) \right\rceil + |F_u^v|,$$

where $|F_u^v| = 2^u$! — power plurality of group transformation; HCCDUC for extended codes:

$$l_{K_+} = (1/2k - 1/2k) \left\lceil \log_2 (2\sqrt{q} + q + 1) \right\rceil + |F_u^v|.$$

Table 3.21 in Fig. 3.31 these results cracking complexity decoding algorithm rearrangement in different $GF(2^m)$.

Table 3.21. — Dependence difficulty breaking HKKKUK over $GF(2m)$

$GF(2^m)$	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	2.786	2.835	4.122	4.257	1.089	1.864	2.391	3.46
2	4.978	5.961	6.233	6.781	2.569	3.643	4.108	4.962
3	7.568	8.120	8.234	9.764	3.57	4.131	5.382	7.623
4	9.87	12.1	12.647	13.32	4.92	5.817	6.836	8.972
5	12.017	14.224	14.742	16.892	7.591	8.617	10.13	12.005
6	14.983	17.483	18.767	19.76	10.85	12.53	14.673	14.962

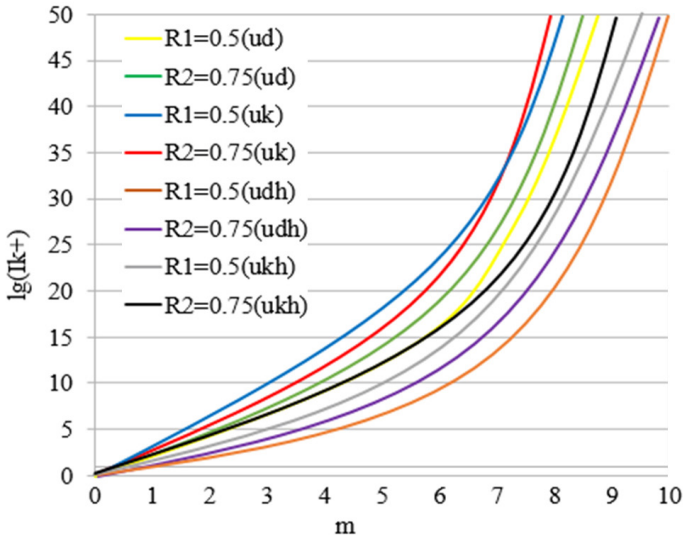


Fig. 3.31. Dependence difficulty breaking HCCDUC over $GF(2m)$ (Permutation decoding)

The obvious result is a reduction in the power field, as demonstrated Tab. 3.21 and graph in Fig. 3.40 further reduce the complexity of breaking, which is shown by subsequent statistical tests, it is offset by a universal compression algorithm MV2.

Difficulty forming codogram determined expressions:

for HCCDUC truncated at MEC: the implementation of a systematic coding is given by: $O_K = (r+1) \times (2\sqrt{q} + q + 1 - 1/2k) + O\left(\frac{1-K_C^u}{K_f} \times L\right)$, for non-systematic coding:

$$O_K = O_K = (k+1) \times (k+1) \times (2\sqrt{q} + q + 1 - 1/2k) + O\left(\frac{1-K_C^u}{K_f} \times L\right). \quad (3.86)$$

For HCCDUC extended to MEC: the implementation of a systematic coding is given by:

$$O_K = (r+1) \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k) + O\left(\frac{1-K_C^u}{K_f} \times L\right). \quad (3.87)$$

For non-systematic coding:

$$O_K = (k+1) \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k) + O\left(\frac{1-K_C^u}{K_f} \times L\right). \quad (3.88)$$

The difficulty decoding codogram determined by the expressions:

– for HCCDUC truncated at MEC:

$$O_{SK} = 2 \times (2\sqrt{q} + q + 1 - 1/2k)^2 + 1/2k^2 + 4t^2 + (t^2 + t - 2)^2 / 4 + O\left(\frac{\alpha - z \times \log k}{|K_z^c \times L|}\right); \quad (3.89)$$

– HCCDUC extended for at MEC:

$$O_{SK} = 2 \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k)^2 + k^2 + 4t^2 + (t^2 + t - 2)^2 / 4 + O\left(\frac{\alpha - z \times \log k}{|K_z^c \times L|}\right). \quad (3.90)$$

The complexity of the task analysis (decoding) define the expressions:

– for HKKKUK truncated at MEC:

$$O_{K+} = N_{pokr} \times (2\sqrt{q} + q + 1 - 1/2k) \times r + N_{Fabo}(N_K), \quad (3.91)$$

where: $N_F \approx \frac{K_C^z}{2^{1-K_C^{z+1}}} \times |F|$; $K_C = 97/128$, $|F|$ — the total length of the output flags (losses) (bps) — a known attacker residue (unprofitable text) and set the flag (loss) of the unknown keys — $N_K \approx 2^{1190 \times z}$, $z = 16$;

– HCCDUC extended for at MEC:

$$O_{K+} = N_{coating} \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k) \times r + N_{Fabo}(N_K). \quad (3.92)$$

Table 3.22 in Fig. 3.32 shows these results fracture complexity and difficulty of coding for different velocities in different $R GF(2^m)$. Table 3.23 in Fig. 3.33 these results depending on the amount of public key data on HCCDUC MEC for different indicators of sustainability.

Table 3.22. — Difficulty fracture and complexity of coding for different velocities R

$lg(I_s)$	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

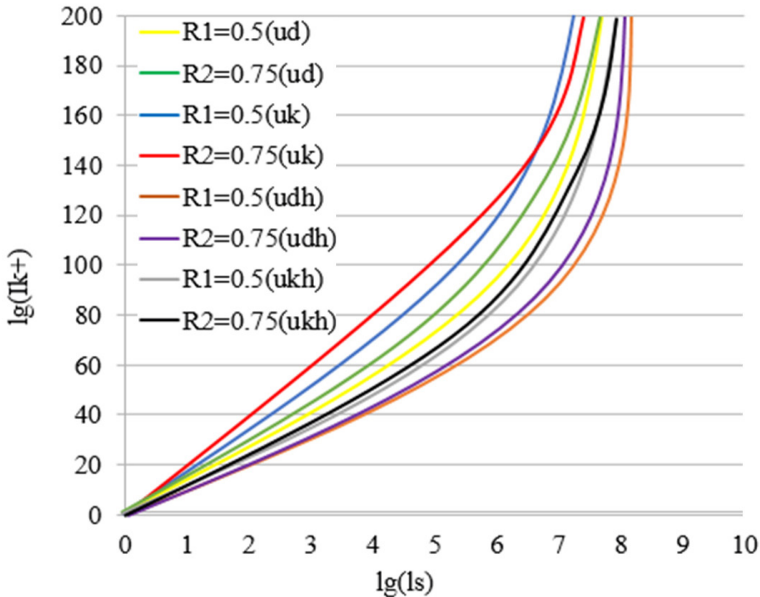


Fig. 3.32. Overall chart fracture complexity and difficulty of coding HCCDUC

Table 3.23. — Dependence of public key data HCCDUC the indicator of stability

$lg(l_{k+})$	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

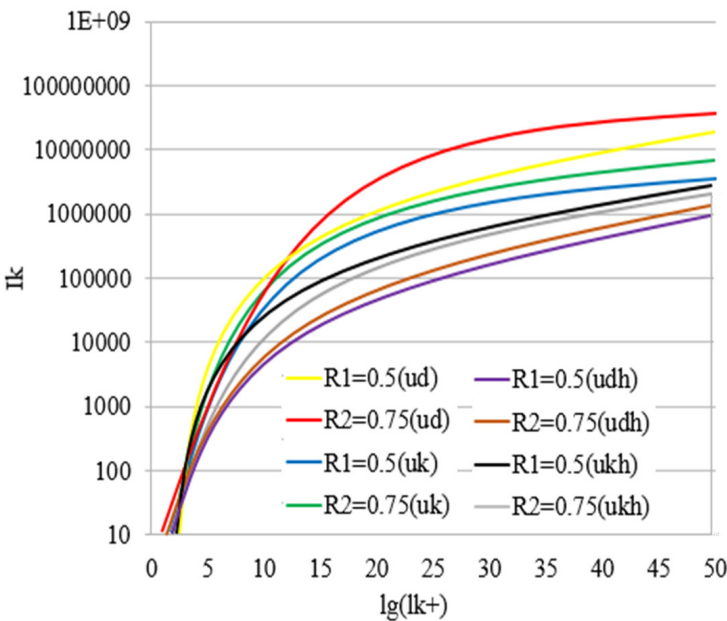


Fig. 3.33. Dependence of public key data HCCDUC the indicator of stability

Table 3.24 the results of researches at the capacitive characteristics of program implementation capacity field.

As the study received a significant reduction MNCCS public key data HCCDUC, which leads to an increase in the total relative speed transmission.

A natural continuation of research must obviously be testing the statistical characteristics of the offered crypto-code constructions in order to obtain objective data on their traditional cryptographic immunity and comparison with known algorithm.

For statistical stability studies investigated use cryptographic package NIST STS 822 [47]. The research results are presented in Table 3.25.

Table 3.24. — Dependence of software implementation of the power field
(Number of group operations)

Crypto-algorithms	2⁴	2⁵	2⁶	2⁷	2⁸	2⁹	2¹⁰
MacElis truncated at <i>MEC</i>	8293075	10007947	17787431	28595014	44079433	61974253	79554764
MacElis extended to <i>MEC</i>	8506422	11156138	18561228	33210708	48297112	65171690	84051337
HCCDUC on MNCCS MacElis extended to <i>MEC</i>	5612316	7900315	14892945	25565274	42279183	58963778	76564173
HCCDUC on MNCCS MacElis truncated at <i>MEC</i>	5942627	7905257	14682411	25595014	42116327	58468143	75474764

Table 3.25. — The results of statistical studies of safety

Cryptosystems	Number of tests, which have been tested more than 99 % sequence	Number of tests, which have been tested more than 96 % sequence	Number of tests, which were tested at least 96 % sequence
NCCS MacElis	149 (78.83 %)	189 (100 %)	0 (0 %)
MNCCS MacElis truncated at <i>MEC</i>	151 (79.89 %)	189 (100 %)	0 (0 %)
MNCCS MacElis extended to <i>MEC</i>	152 (80.42 %)	189 (100 %)	0 (0 %)
HCCDUC extended to <i>MEC</i>	153 (80.95 %)	189 (100 %)	0 (0 %)
HCCDUC truncated at <i>MEC</i>	155 (82 %)	189 (100 %)	0 (0 %)

Table 3.25 showed that despite the decrease in the power field Galois to $GF(2^6)$ for MNCCS and $GF(2^4)$ for HCCDUC statistical characteristics of crypto-code constructions were at least no worse than traditional NCCS McEliece in $GF(2^{10})$. All cryptosystem tests were 100 %, and showed the best result in shortened HCCDUC MEC: 155 189 tests completed at 0.99, which is 82 % of the total number of tests. This traditional NCCS McEliece in $GF(2^{10})$ 149 tests showed at 0.99.

Thus, the proposed methods of providing basic services security SI, confidentiality and integrity enable integrated to provide the necessary level of stability and reliability BI in ABS.

Consider the proposed method of ensuring data authenticity through HCCDUC McEliece and Niederreiter.

3.3 Develop methods to ensure the authenticity of the bank in automated banking systems based on two-factor authentication hybrid crypto code structures with unprofitable codes

3.3.1 Research protocols two-factor authentication

According to international standards ISO 7498, ISO/IEC 10181 to provide the necessary safety parameters identified five basic conventional services, the main ones are only two: the authenticity and integrity, to ensure their security mechanisms are used, most of which are implemented based on cryptographic techniques conversion information.

The main mechanisms to ensure integrity and authenticity of information in the Air Force at different levels based on the use of standards symmetric block cipher (3DES, GOST 28147–2009). Examples of program implementation mechanisms are discussed software cryptographic protection “Griffin B” and “Griffin L” intended for cryptographic protection of confidential information in automated banking systems [48, 49]. The main characteristics of data security software are listed in the Table 3.26.

Software tool “Griffin B” is for cryptographic protection of confidential information in the automated banking system and is used for sharing information within a corporate network bank clients who work with the system “Client-Bank” systems servicing plastic cards [48]. The software cryptographic protection of information “Griffin L” [49] is intended for use in banking, in particular for the exchange of confidential (including financial) information within the corporate network of the bank, with customers working on the system “Client-Bank” systems servicing plastic cards and others.

Table 3.26. — Key Features of software protection

Specifications	“Griffin B”	“Griffin L”
Key features applications	Test hash, including Encryption simply replacing; Getting the numbers p , q (512 bits and 1024 bits); Test creation and verification of electronic signature; Performance Tests (encryption, hash, generation number, CPU); Simple and targeted encryption string or file; Hash string or file; Generate wide setting; Generate user key; Changing the password on the secret key; Signature line or file; Total private key algorithm Diffie-Hellman	
Standards	GOST 28147–2009. Algorithm cryptographic transformation; GOST 34.311–95. Hash function; GOST 34.310–95. The procedure for making and verifying digital signatures based on asymmetric cryptographic algorithm. Scheme key distribution Diffie-Hellman. Standard X9.17 to generate session keys.	
Performance on a PC with a processor 633 MHz delivers	the memory encryption mode easy replacement – at least 5 MB / s; hash the memory – not less than 1.5 Mb / s; CPU computing - no more than 0.015 seconds; CPU test – no more than 0.020 seconds; generation common key for Diffie-Hellman method – no more than 0.015 sec.	the memory encryption mode easy replacement – at least 2.5 MB / s; hash memory area – at least 1 Mb / s; CPU computing with key length of 512 bits – no more 0.02 s; CPU test – no more 0.03 s; generation common secret – less than 0.02 sec.

Thus, to ensure the authenticity of the SI in ABS using symmetric and asymmetric crypto algorithms, digital signatures and hash functions based on MAC and MDC-codes [4, 11, 13, 14, 15, 23, 25, 26].

To ensure authenticity in financial services in the creation of Internet banking, mobile banking, usually using electronic signatures based on multifactor authentication or extended. It is based on the combined authenticator, divided physically, which significantly increases the safety of use, at least on the part of

users accessing information systems in protected and unprotected communication channels.

Two-factor authentication, or 2FA — a method of user identification in any service that uses two different types of authentication data. The introduction of an additional level of security provides better protection against unauthorized account access. Using this type of 2FA, the user enters the first level of authentication personal password. The next step, he must enter the OTP token (OTP — One-time Password Algorithm), usually sent by SMS to his mobile device. OTP will be available only to those who are supposed in theory, introduced the available third-party password [50, 51]. Methods strict (two-factor) authentication is often used in the financial sector, but in principle can be applied in almost any other field. The main methods of construction of two-factor authentication classified [54]:

1. Software to identify a specific computer. In computer installed a special program that sets it a cryptographic token. Then, in the authentication process will involve two factors: the password and token embedded in a PC. Since the marker is always on the computer, the user login only need to enter a user name and password.

2. Biometrics. The use of biometrics as a second factor of authentication is done by identifying the physical characteristics of the person (finger print, eye membrane, etc.).

3. Disposable e-mail- or sms-password. Use as a secondary factor authentication password OTP, perhaps by sending the second one-time password to the registered email address or mobile phone.

4. Token with a single password. User is a device that generates a constantly changing passwords. These passwords entered by the user in addition to your regular password when authenticating.

5. Control outside. This method involves a call from the bank at a pre-registered phone number. The user must enter the password on the phone, and only then he will get access to the system.

6. Identification using gadgets. Such identification is performed by placing cryptographic tag to any user device (e.g. USB-drive, iPad, memory card, etc.). When registering, the user must connect the device to a PC.

7. Card with a layer. The user is issued a card with PIN-code is used only once.

General classification methods multifactor authentication shown in Fig. 3.34.

Given in [6, 8, 10, 52] multifactor authentication methods analysis showed the following major advantages and disadvantages:

The advantages of the methods based on SMS — you notifications OTP generation-codes at each entrance and transfer to additional channels, intercept login and password on the main channel will not lead to the attacker bank

client information. Binding OTP-password to the phone numbers. The main disadvantages are: use of open channel provider can not provide confidentiality OTP-codes using only cellular channels leads to “losing” two-factor authentication. There is a theoretical possibility of substituting numbers across service provider or employees mobile shops.

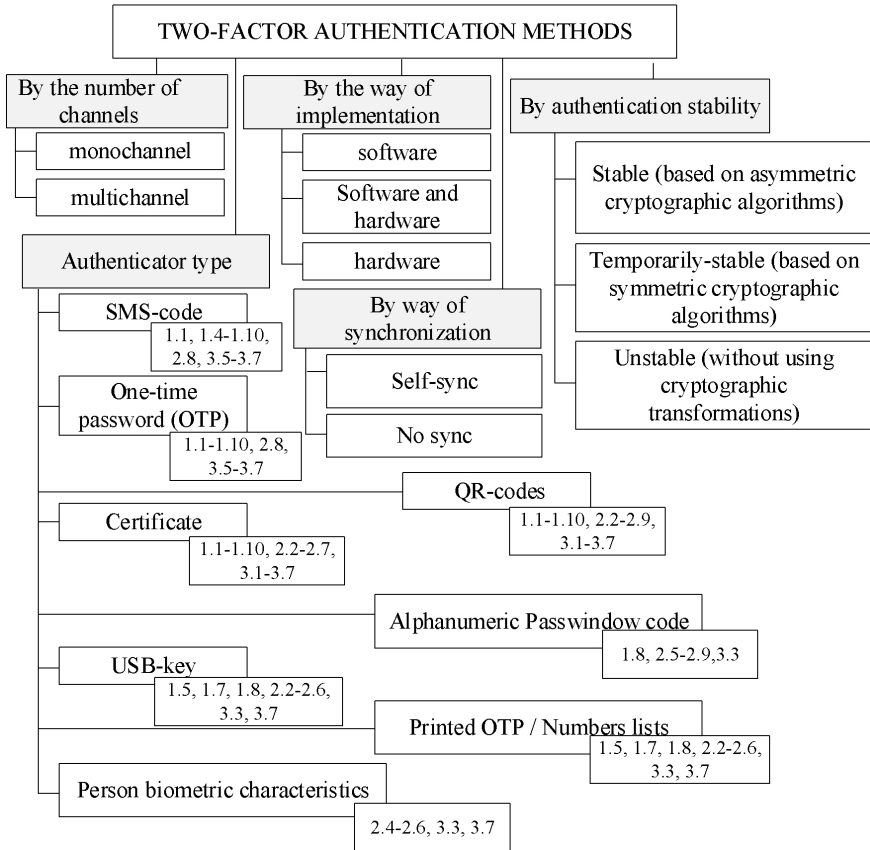


Fig. 3.34. Multifactor authentication methods classification

– Using methods of extra-authenticator (QR-codes) can support multiple accounts in a single authenticator and create a primary key, no need to use cell lines, OTP generation>Password-based encryption algorithms. The main disadvantages are — authenticator using the same device from which the entrance leads to a “loss” two-factor access to primary attacker user key leads to cracking the authentication system.

– Check the log using mobile applications automates the authentication process without user verification based private key authentication in the mobile

application. The main disadvantages are: loss/private key disclosure results in cracking the authentication system, the possibility of receiving SMS-messages through synchronization between iPhone and Mac, use authenticator on the same device from which the entrance leads to a “loss” multifactorial.

- Physical (or hardware) tokens is the most reliable method of two-factor authentication. Often they are presented as USB-sticks with its own processor, which generates cryptographic keys that are entered automatically when connected to a computer. The advantage is the absence of an additional mobile applications, software, tokens are completely independent device. The disadvantages include- using multiple accounts leads to “bundle” tokens that are not supported by all applications.

- Back keys are spare option in case of loss/theft of smartphones, which come one-time passwords or codes confirmation. Loss/theft of keys reserve leads to destruction of privacy authentication system.

- Bar-Passwindow system codes provide unique static image sequence of characters generated dynamically authentication server without encryption algorithms. Any-interference pattern or fake bar-code is passively presented to the user in the form of combinations appearance in a pattern that does not meet expectations. A major drawback is the possibility of a unique selection bar-code card proposed in [6].

- The use of biometrics as a secondary factor authentication is done by identifying the physical characteristics of the person (fingerprint, iris, etc.). Advantages of the method is to use the unique physiological characteristics of the person, the absence of additional mobile applications and software. A major drawback is the specific requirements for software-hardware devices readable biometric user data.

Thus, in automated banking systems are generally used multifactor authentication systems based on one-time e-mail or sms-password and different types of tokens. To ensure privacy standard remote banking OTP Bank transferred- must use encrypted codes and independent operators channel delivery. This approach is not subject to the majority of known threats, in addition to social engineering that exploits the human factor.

3.3.2 Analysis of the threats that are relevant for today's two factor authentication protocols

The analysis of threats [61, 62, 63, 64, 65, 66] indicates a significant transformation and their hybridity. From a purely threats IS, CB, SI infrastructure ABS, displays signs of hybridity threat began to occur as a result of simultaneous action on the object of protection — SI in ABS by the emergence of the phenomenon of synergism [61].

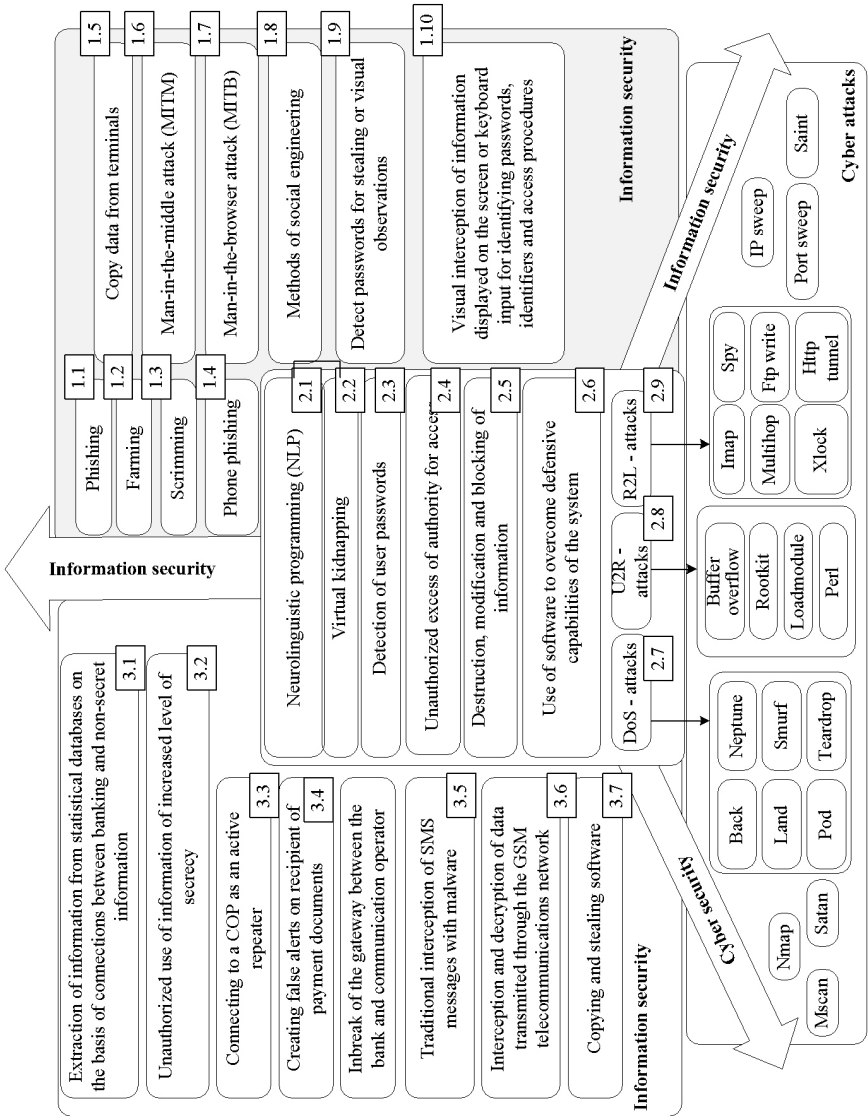


Fig. 3.35. Synergetic model of banking information security threats

Fig. 3.35 shown synergistic approach to classifying threats multifactor authentication combined with shown in Fig. 3.34 2 classification methods FA.

Analysis of current authentication systems showed that their safety is measured by dividing the difference between the cost benefit attacks and for attacking the cost of protection against them. So expensive, although safer methods such as cryptographic PKI-protected devices with their own channels, screens and keypads are rated so low on a scale of security, while the banking system is still largely based on the cheapest and seemed be the least secure method of using PIN-codes and passwords. Total cost and complexity of deploying such devices often outweighs the benefit of their extremely high security.

Threats to the security of the network ABS can be divided into network attacks (information coming from the remote agent) and local attacks originating from malware already installed on the client system, such as Trojans, rootkits, and so on. Often authentication security assessment focused primarily on network attacks suggesting that the terminal (ie, desktop computer, laptop or mobile device) is protected platform [5, 50, 51, 52]. However, often the attacker has full access to the victim's computer through the hidden processes of communication that remained from malware using uncorrected security holes licensed software.

Typical methods of attacks on Bing are:

- Fracture online databases — stealing information stored in commercial databases, data.
- Man in the middle/phishing — third party intervenes and represents the client and server, making recording and/or alter each other.
- Attacks in social engineering — cheating customers with a view to find out their personal information for transmission by hackers.
- “Man in the Browser” — malicious software that is installed on the computer victim to report network activity, keystrokes and screen data captured by a hacker, allowing him to intercept data transfer funds, which funds may be unintentionally distorted by changing the information displayed in the browser user.
- Attack with full-force passwords — polled the server with all possible combinations of passwords.
- Simple theft — written details about authentication or card can be physically taken and copied.
- Observations from the back — an attacker can quietly watch as the user enters details of the transaction.

With the proliferation of GSM, smartphones and tablets connected to the network, even this safety advantage can be lost if user authentication transactions

carried out on the same mobile device. In addition, the growth of unwanted software for mobile now allows an attacker to gain access to the authentication codes sent via SMS not only through traditional means of interception by malicious software [55]. But by intercepting and decrypting data transmitted via GSM-network telecommunications [57].

Attacks mobile authentication successfully conducted without such technology. Instead, an attacker impersonating a user device and asks that all SMS messages sent to another phone number throughout the attack [57]. Another method of authentication using mobile camera to read the barcode image on a workstation user who encrypted with OTP information about the transaction. This method has a problem, assuming that the operating system on the mobile device is not subject to such a vulnerability to malicious software, like all other forms of software that works with the network [59].

When using biometric authentication user data available for online authentication. However, biometric authentication devices can not communicate with local devices or network without facing malware attacks and/or attacks “mediator” [56]. This method is as impossible to change again, after the attacker gave himself for user using biometric authentication.

Biometric authentication provides the user with a convenient way to generate online user name, but the network and tapped the infected mobile device, the overall performance of the safety of such methods is better than using normal user name and password.

Electronic hardware tokens come in several forms and include various security features authentication. The most common hardware tokens generating one-time passwords (OTP) using cryptographic algorithms with an internal key, or, more often, the secret key is generated based on common, synchronized system time values. The user device reads the displayed numbers and manually enters them into their terminals to cross-reference with the authentication server.

This simple method of electronic OTP generation remains vulnerable to attacks “mediator”, as users are required to disclose OTP no means of checking the authentication context.

In response, many manufacturers have added a small token numeric keypad, significantly increasing the size of the marker, but allowing the user to enter information about specific transactions encrypted with a secret key before the user enters the result in his terminal. This is a type of check or signing a transaction and does provide some protection from attack “mediator”.

However, this method is still vulnerable to attacks using laborious manual process of signing the transaction. The time and attention required to perform

manual operations have been successfully used to distract the user from the transaction context information that the user takes, and therefore attacks can be successfully implemented on a mass scale [60].

Printed lists OTP/grid numbers. The older method of providing one-time passwords — a printed list of randomly generated passcodes or transaction authorization codes on paper or scratch cards. Each access code is requested in sequence and is used to authenticate a transaction.

An alternative may be used printing character and authentication server will issue a barcode, asking symbols are in certain coordinates.

Both methods use the keys and signals that can be communicated verbally. This allows the attacker to ask the user follows the actual code via malware using social engineering or phishing attacks. In addition, the relatively low entropy lists or grids require frequent changing of keys to prevent repetition code request attacker.

These methods are vulnerable to the full range of attacks “intermediary” for the same reasons that all authentication methods with unknown context.

Fake (weakened) barcodes. An attacker could try to weaken the protection PassWindow, changing the frame rate of this (intercepted) bar code before delivering weakened (Simplified) barcode person. This method reduces the entropy of the bar code to change the details that would facilitate analysis intercept requests/responses. But obviously damaged barcode passively warns the user attempted attack, causing suspicion about the use of computers and communication channels.

This attack requires a large number of hacker steals from 20–30 in the case of small templates for hundreds of large templates of several thousand when using the method in the animated Advanced Security.

Consider an effective method of breaking two-factor authentication based on PassWindow.

3.3.3 Use two-factor authentication based on PassWindow and analysis of safety

PassWindow is a way to provide two-factor authentication in the online environment. It includes two matrix — a physical key with patterned printed on plastic portable digital pattern plate and bar code represented as an image on a standard electronic screen, for example, the display laptop or mobile device. They generate a unique one-time password to the user and a set of numbers for a single transaction when overlapping. This password is then used for online authentication and authentication transactions. Information about specific transactions included in these figures, such as the intended account number or

transaction amount, allowing the user to visually confirm the authenticity of the received authentication request [67].

Technology PassWindow based on the unique ability of the matrix to transmit information so that it stands only at imposing physical pattern of signs intended recipient (the information the user has) and then displays a template bar code (challenge pattern) electronic network devices users such as computer, smartphone, and so on. The combination of the key and template barcode coded information shows only a single user, and a complete revision of the template is possible only with the direct angle. Any interception barcode via electronic devices means that information when no leak is enough to have learned the secret key attacker template user for the duration of the card.

Patterns barcode PassWindow may exist as unique static images or sequences of characters in a more extended version of the animation, which is the main subject of this document. These animated barcodes consist of a sequence of static templates, each containing coded characters or mean nothing and just add dynamic entropy in the whole pattern [67]. Sequences templates barcode dynamically generated authentication server so that each is unique (and, therefore, make sense) only in conjunction with the key to which they are suited. The main stages PassWindow system shown in Fig. 3.36.

The analysis in [6] threats PassWindow showed that the most effective analytical threat is an attack on a secret key (barcode card). To succeed algorithm should take three to five sessions monitoring (transfer client OTP Bank). Monitoring algorithm plastic cards PASSWINDOW shown in Fig. 3.37.

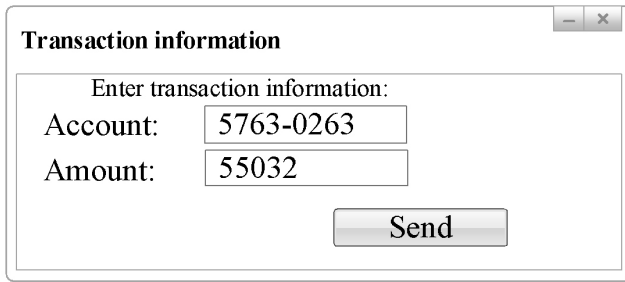
In the interest of testing PassWindow vulnerability to such attacks, was built fracture algorithm that tries to use these principles to perform this analysis, which confirms the practical part of the algorithm regardless of the number of transferred numbers.

Monitoring algorithm based on plastic cards PassWindow system consists of the following steps (see Fig. 3.37):

1. Monitor channel and receive data sessions.
2. Translation of data into a class indicator (in the form of binary code), which is able to operate as an object (class indicator represents an array of 7-units/zeros);
3. Check the possibility of forming “numbers” in each item card (loop for all sessions). Inside the loop cycle begins for each sequence — turns every indicator seems “true” (believe it was the figure).

Inside the loop is checked — if the current position is “true”, then the option is created, which is recorded reverse indicator generator if the position is “wrong” — written indicator. After each cycle within a sequence is the intersection of the last sequence variants, i.e. $N_i \cap N_j$ — final leaves (variants) are reviewed and thrown up;

1. The users enters transaction information for authentication



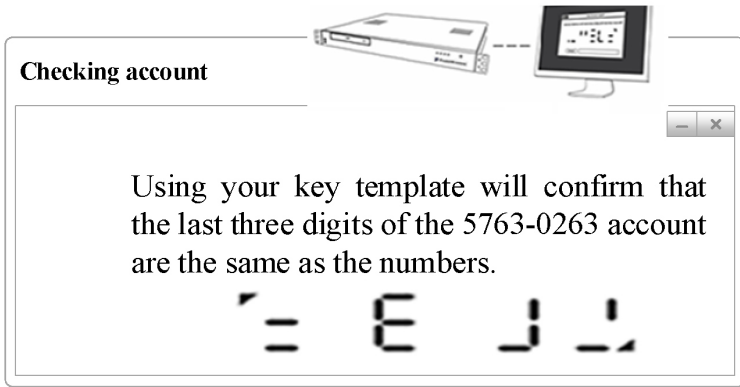
Transaction information

Enter transaction information:

Account:

Amount:

2. After this, the PassWindow authentication server creates a single-use barcode and also specific information: the last three digits “263”

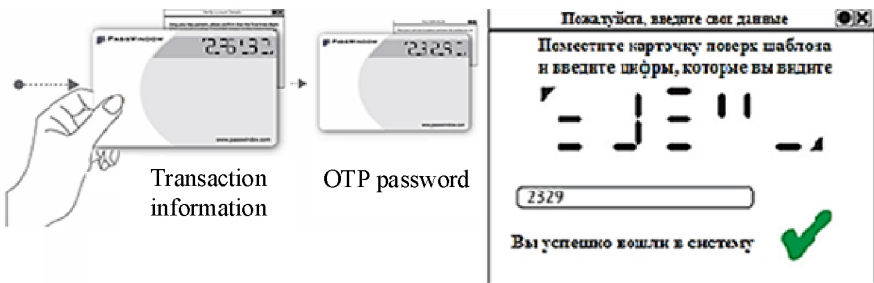


Checking account

Using your key template will confirm that the last three digits of the 5763-0263 account are the same as the numbers.

' = E J J

3. The user puts a card with the key and visually checks the transaction information coincidence; after that, he enters a one-time password to authenticate the transaction.



Transaction information

OTP password

Пожалуйста, введите свои данные

Поместите карту поверх шаблона и введите шифры, которые вы видите

' = J E J J

Вы успешно вошли в систему

Fig. 3.36. The main stages of PassWindow

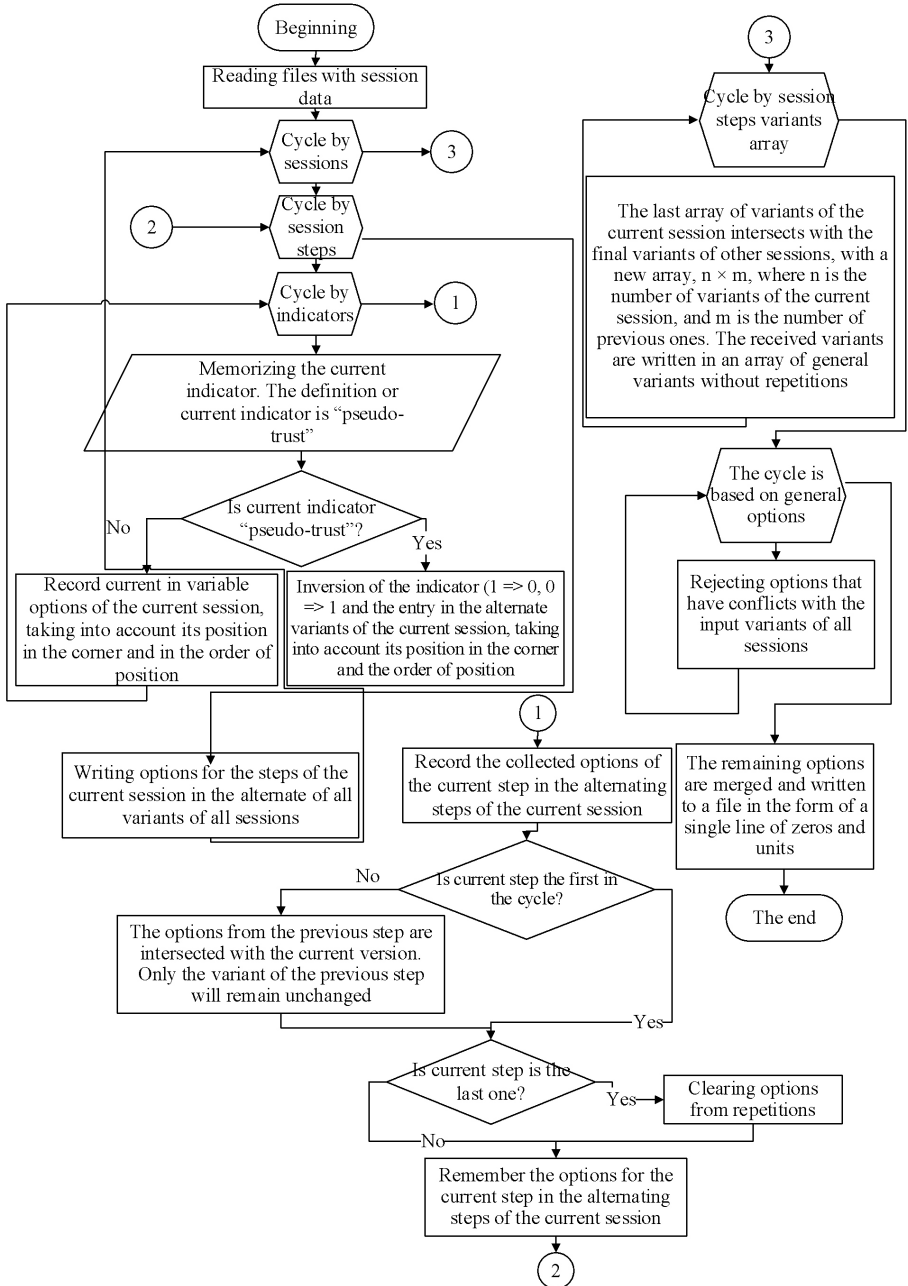


Fig. 3.37. Algorithm monitoring system PassWindow

4. Review all sequences in all sessions. Intersection of letters between sessions alternately (first session of the second, the result of the intersection of the third session and so on. D). After each session intersection adjacent leaves — leaves “exempt” from the copies;

5. Intersection of letters sessions together. Cycle all letters — each option is checked for incoming data — the data generator, if it has a conflict which indicators, such sheet (option) is discarded. As a result, there will be only one option that does not conflict with any of the sequences of all sessions;

6. Conclusion of the final version of a file output.txt binary string format.

The proposed algorithm PassWindow monitoring system allows the transmission of 3–5 sessions OTP password generate unique barcode card user and get full access to its bank accounts.

3.3.4 Research methods for constructing OTP password

Trends in ABS lead to the fact that users must use different devices to access the resources of financial services ABS — used stationary or mobile computer, tablet or smartphone [15, 68]. Technology-time password (OTP), can help implement a strict two-factor authentication, and requires significant costs of implementation and support [15, 68]. OTP virtually invulnerable to attack the network analysis package, and further requires the user to enter a PIN-code, which is an additional factor of authentication [15, 68]. Thus, a two-factor user authentication system based on the possession of something (Authentication by Ownership) or based on knowledge of something (Authentication by Knowledge) [68]. The downside of using OTP-password is the ability to “intercept” malicious text (SMS-messages) from one part of the token. Attacking may compromise your 2FA based on text in several ways: based on the methods of social engineering (forwarding messages through ISP) intercept messages using the IMSI-catcher (International Mobile Subscriber Identity — international identification of mobile subscribers), using flaws in the protocols that allow operators due to exchange data between networks [69, 70]. For this reason, the National Institute of Standards and Technology USA (NIST) in [71] prepared to ban the use of two-factor authentication based OTP-passwords for services that are connected to the public IT systems. Thus, there is a contradiction between the OTP-use passwords and protocols two factor authentication security for their use.

In [71], the following authentication confidence level (Authenticator Assurance Levels, are shown in Fig. 3.38.

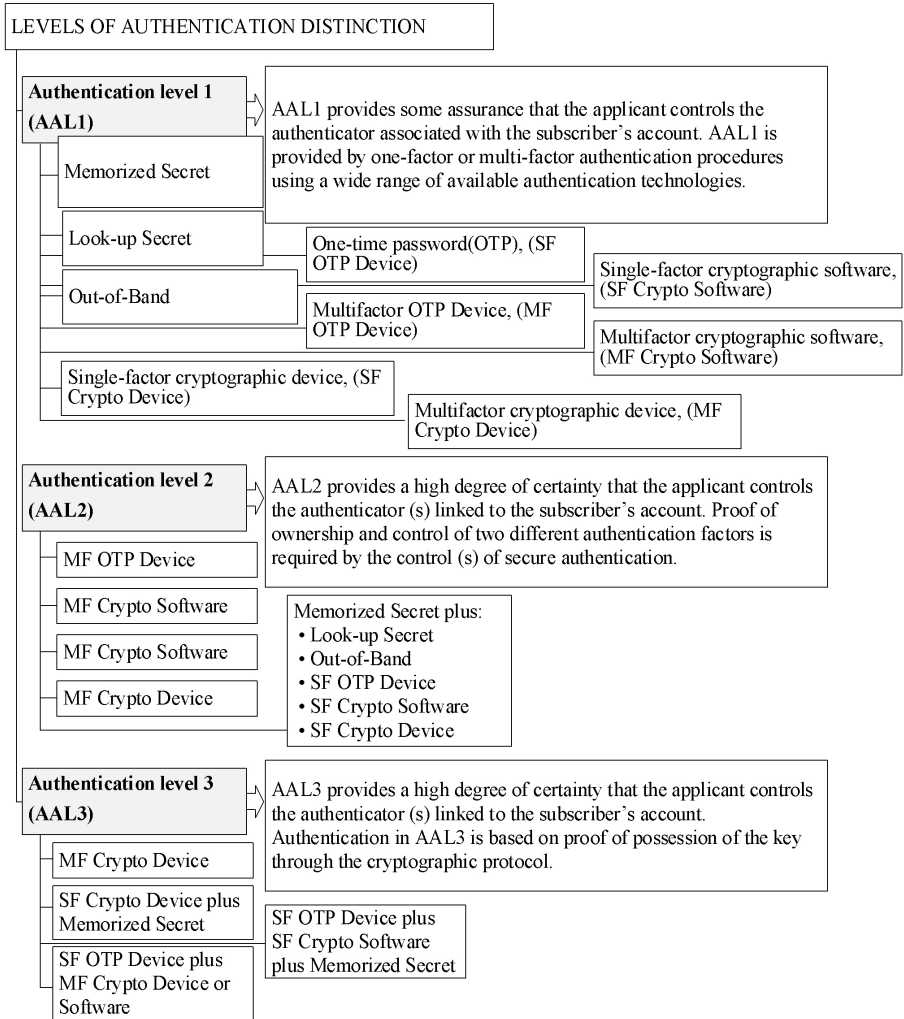


Fig. 3.38. The levels of reliability and authentication mechanisms of OTP password

The analysis of requirements in [71, 72, 73, 74] to OTP-forming methods passwords showed that:

- secret authenticator memorable — commonly called password or if numeric, PIN — a secret meaning that for selecting and storing user must consist of 8 characters, be very difficult to remember and kept secret. To form a secret authenticator proposed to use algorithms of MAC codes: HMAC [FIPS 198–1], SHA-3 [FIPS 202], CMAC [SP 800–38B] or KMAC Message Authentication Code (KMAC), customizable SHAKE (cSHAKE) or Parallelhash [SP 800–185];

- secret authenticator Look-Up — represent a physical or electronic record, which stores the set of secrets that are shared between the applicant and CSP (Center for Security Policy — Center for Security Policy). To create the list of secrets standardized random bit generators [SP 800–90Ar1] [74];

- authenticator-band — the physical device that uniquely addressable and can communicate securely with the verifier through a separate channel, called the secondary channel. The device has also supervised the applicant and supports private communications by the secondary channel, separate from the primary channel for electronic authentication. To form the second channel can be used by public network, dial (4G LTE). Authenticator is transmitted in encrypted form [75];

- single-OTP-generating unit OTP. This includes hardware devices and software generators OTP, installed on mobile gadgets. These devices have built-in secret, which is used as a key for OTP generation and requires activation via a second factor. To generate the key using symmetric and asymmetric crypto algorithms. OTP is displayed on the device and entered manually for transfer to the verifier, thus proving ownership and control device;

- multi-device generates OTP for use in authentication after activation with an additional authenticator. The device uses hardware devices and software OTP generator based on symmetric encryption algorithms or hash functions that are installed on mobile gadgets. The second factor authentication can be achieved by using a built-in input area integrated biometric reader (e.g. fingerprint) or direct computer interface (e.g. USB-port). OTP is displayed on the device and entered manually for transfer to the verifier;

- single-factor authenticator encryption software — a cryptographic key stored on disk or some other “soft” media. Crypto-factor authenticator software encapsulate a secret key that is unique to the authenticator. Authentication is performed by checking the ownership and control key;

- single-cryptographic device is a hardware device that performs cryptographic operations using secure cryptographic key and providing output authenticator via direct connection to the endpoint user. The device uses a built-in symmetric or asymmetric cryptographic keys and requires activation via a second factor of authentication. Authentication is performed by checking the ownership of the device authentication protocol;

- multi authenticator encryption software — a cryptographic key stored on disk or some other “soft” media that requires activation via a second factor of authentication. Authentication is performed by checking the ownership and control key;

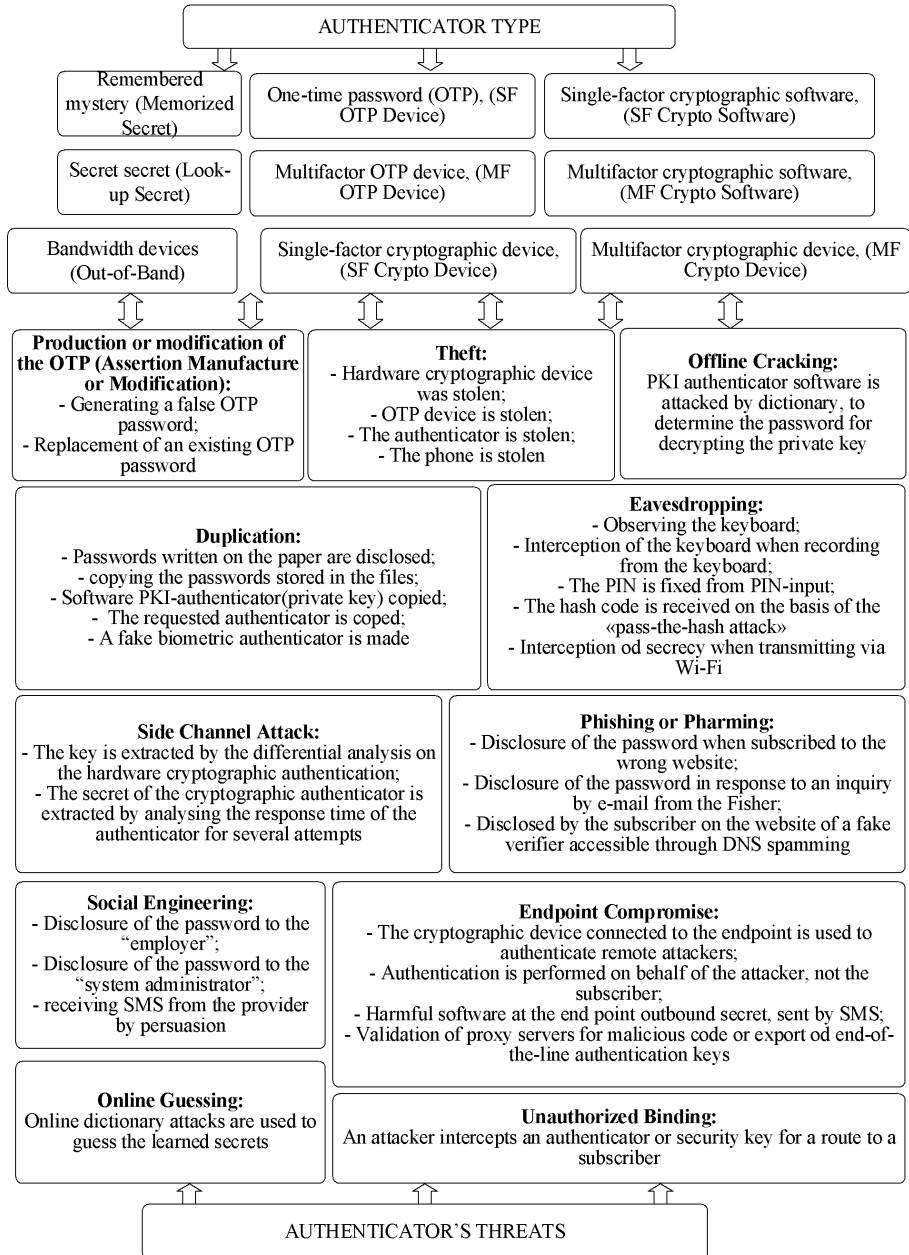


Fig. 3.39. Classification by type of threats authenticator

– multi cryptographic device — a hardware device that performs cryptographic operations using one or more cryptographic keys protected and requires activation via the second content authentication. Authentication is done by checking the device ownership and control key. Exit authenticator provided a direct connection to the endpoint user and depends heavily on the particular device and the cryptographic protocol. Multifactor authenticator devices use cryptographic protected from unauthorized access equipment to encapsulate the secret key.

Fig. 3.39 are the main threats authenticator that can be classified based on the types of attacks authentication factors [51].

The analysis of threats based on a synergistic approach to threat assessment [76] Shows that criminals today use a comprehensive approach to obtain personal data of users and creators service authenticator ABS. Typically, hacking techniques based on combining social engineering techniques with traditional methods of masquerade and penetration.

Also used and new types of cyber attacks to effectively embed malware on mobile communications, which in turn leads to lower profitability multifactor authentication methods based on SMS-messages and passwords OTP-ABS.

Thus, there is need for additional means of transmission authenticator privacy in open systems mobile/4G LTE, dial. In the next section the method of two-factor authentication based on HCCDUC MEC, which can eliminate the contradictions.

3.3.5 Development of two factor authentication protocol on hybrid designs crypto code of unprofitable codes

The analysis attacks on multifactor authentication schemes authenticator using OTP-password allows us to formulate the basic requirements for the following protocols:

- an increase in multi-factor authentication;
- increasing the length of secrets, sustainable use of standard encryption algorithms;
- use encryption procedures in the transmission channels open Internet (GMI), open mobile networks;
- increasing requirements of safety in the system and network devices GMI and mobile networks;
- improving information and cyber literacy users.

To meet the requirements of the authors proposed to use a crypto-code system considered in [7, 8, 9]. In [9, 10] the practical crypto algorithms hybrid coding structures on unprofitable codes that allow improved multi-

authentication scheme to enhance the reliability and reliability authenticator, which is formed.

For this bank card (BC) should keep the following data elements [8, 10]:

1. Index of public key certificate authority — so that the terminal can handle multiple certification centers, this value specifies that the keys must use the terminal when working with this card;
2. the public key certificate issuer — signed by the Certification Center;
3. Public Key Certificate BC — signed by the issuer and is based IAMB McEliece;
4. module and the public key exponent of the issuer;
5. module and the public key exponent BC;
6. The secret key BK.

The terminal that supports multifactor authentication scheme, should keep public keys of all CAs and associated information related to each of the keys.

The terminal should also be able to choose the appropriate key index based on (1) and some special identity.

To support multifactor authentication bank card (BC) the user should have its own key pair (public and private key authenticator). The public key is stored on the BC in BC public key certificate. Each public key BC certified by the issuing bank, and trusted certification authority certifies the public key of the issuing bank. This means that the authenticator to verify the card terminal must first check the two certificates to authenticate and restore BC's public key, which is then used when checking authenticator BC.

The process proposed authentication method consists of five steps:

1. Restore the terminal public key certificate authority. The terminal reads the code (1) identifies and extracts the module public key certificate authority stored in it — masking matrix (X, P, D) , the equation curve geometrical code (AHA) and associated information, chooses the appropriate algorithms.
2. Obtaining initialization vector (secret “places” in the vector error — shortening bits) of the issuing bank. Formation OTP password (error vector based on the modified crypto-code system (MNCCS) Niederreiter).
3. Formation authenticator on the basis of McEliece MNCCS. Getting codeword (authenticator) by adding the received codeword with the session key.
4. Formation of unprofitable text authenticator and loss [40, 41].
5. Check the validity authenticator. Finding a multiplicity of vector errors and comparison of obtained. The structure of the proposed method of two-factor authentication based on HCCDUC shown in Fig. 3.40.

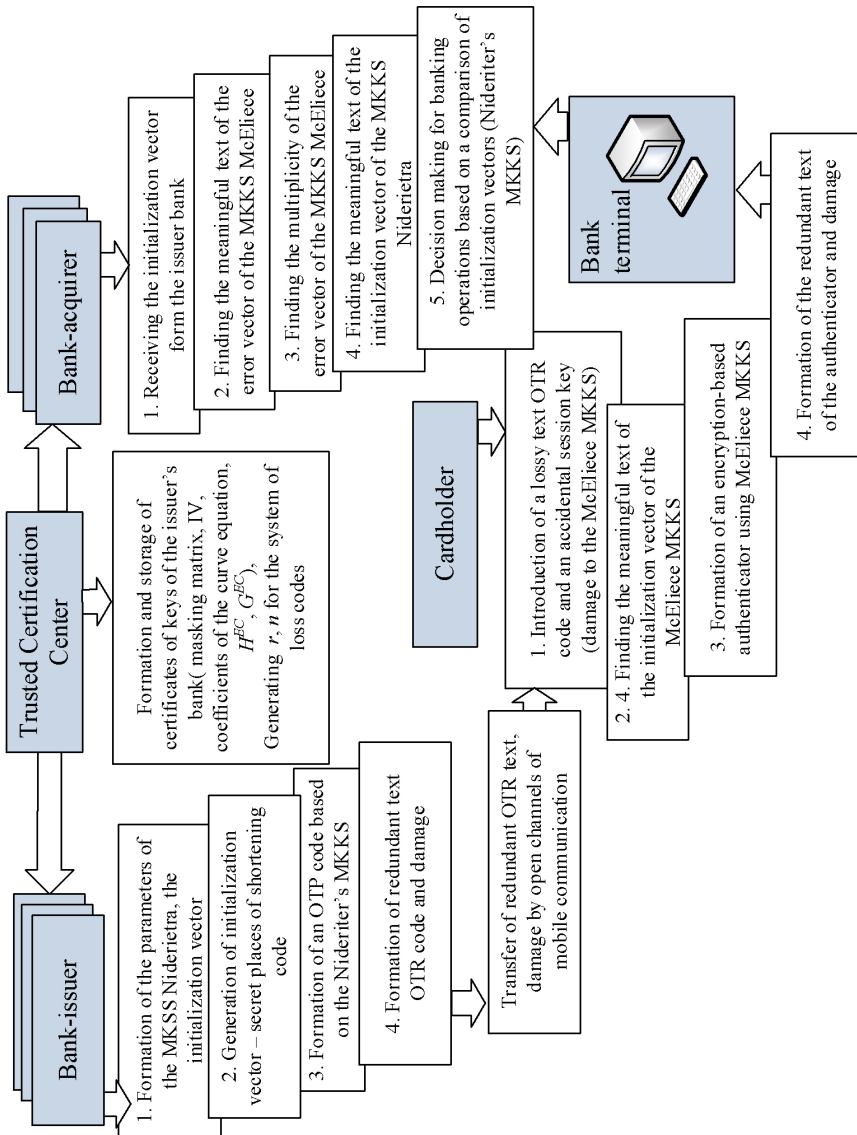


Fig. 3.40. Block diagram of the improved method based 2FA HCCDUC

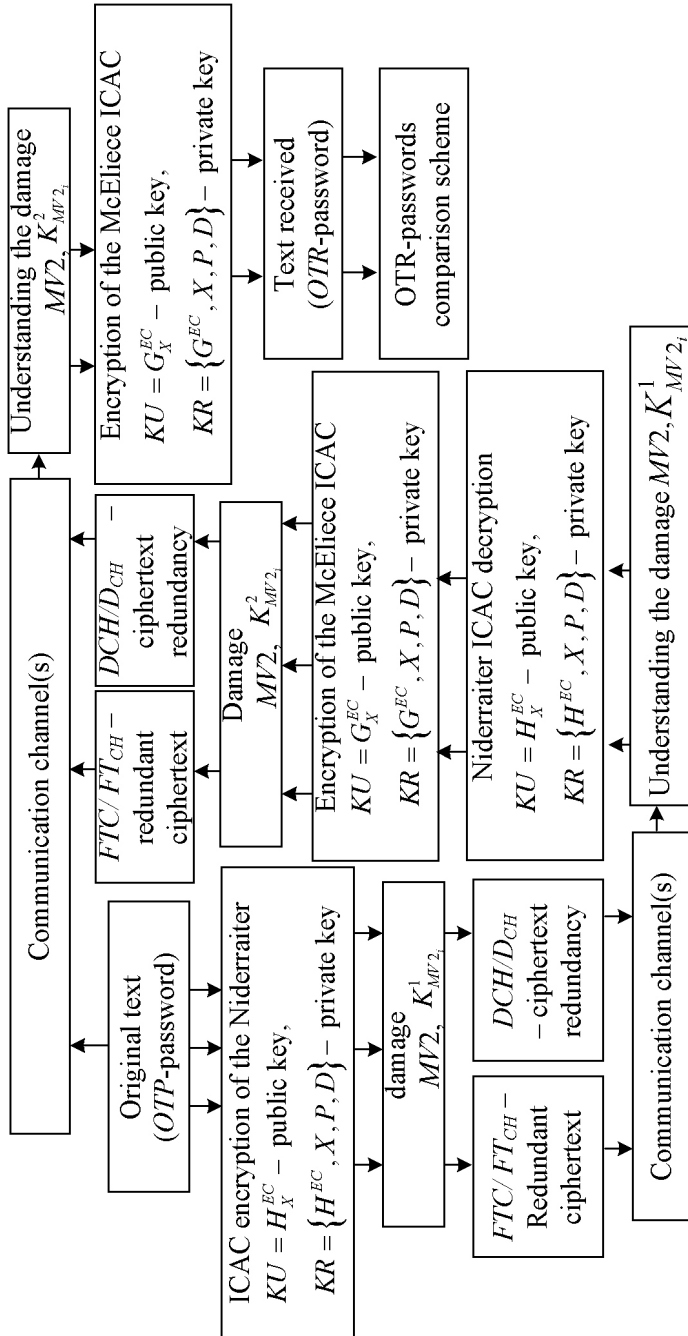


Fig. 3.41. Block diagram of the practical implementation of Protocol 2 to the FA HCCDUC

Thus, hybrid crypto-code constructions on unprofitable codes can increase the number of token authenticator, use two asymmetric crypto-code system, two / four channels unprofitable text authenticator and loss.

Scalable software module by changing the parameters MNCCS Niederaytera and / or McEliece, depending on the requirements put forward communication channel ABS ensures its implementation in mobile gadgets and compatibility with the protocols of Internet banking OPS.

3.3.6 Studying the properties of the proposed method of two-factor authentication

The improved method of rigorous two-factor authentication password OTP-based crypto-code constructions MNKK McEliece and Niederreiter eliminates the main drawback of this protocol 2FA — transfer some token authenticator open channels of mobile communication. Block diagram of the practical implementation of proposed 2FA on HCCDUC shown in Fig. 3.41.

Evaluation of the reliability of the proposed HKKK on unprofitable codes.

To assess the reliability of use proposed in [9] entropy method of reliability assessment.

The proposed hybrid cryptosystem is comparable to the stability of the damage to the second method — damage to ciphertext, considered in [40, 41]. In this case we have a set of ciphertext unprofitable and loss, all individually do not meet the initial meaningful text.

With the full aggregate ciphertext unprofitable and loss of individuality distance is increased due to additional damage to key ciphertext. Thus, additional encryption allows to obtain an increased distance singularity:

$$U_0 = \frac{H(H^{EC}) + H(X_N^{EC}) + H(P_N) + H(D_N) + H(G^{EC}) + H(X_{Mc}^{EC}) + H(P_{Mc}) + H(D_{Mc}) + \sum_{i=1}^m H((K_{MV2_N}^i) + H(K_i)) + \sum_{i=1}^m H((K_{MV2_{Mc}}^i) + H(K_i))}{B \log |I|}, \quad (3.93)$$

where: U_0 — distance individuality;

H^{EC} , X_N^{EC} , P_N , D_N — private key in MNCCS Niederreiter;

G^{EC} , X_{Mc}^{EC} , P_{Mc} , D_{Mc} — private key in MNCCS McEliece;

$K_{MV2_N}^i$ — key in HKKK Niederreiter on unprofitable codes;

$K_{MV2_{Mc}}^i$ — key in HKKK McEliece on unprofitable codes;

$|I|$ — the number of meaningful texts;

B — source code redundancy;
 m — number of losses.

Expression (3.93) to evaluate the stability of the proposed hybrid crypto-code constructions McEliece and Niederreiter on unprofitable codes.

The proposed method provides strict protocol continued use of OTP authentication password, no significant change channels, improve performance software used encryption algorithms that provide hybrid attacks on opposition SI.

3.4 Conclusions of the third section

Thus, in the third chapter of the thesis presents the results of research related to ensuring the confidentiality, integrity and authenticity SI in ABS, including developed and experimentally investigated methods of hybrid crypto-code designs on unprofitable codes (HCCDUC). Based on assessments of the effectiveness TZZI the ABS to ensure confidentiality, integrity BI proposed new mechanisms based HCCDUC that allow you to build asymmetric cryptosystem based on modified asymmetric crypto-code systems (MNCCS) McEliece with modified elliptical codes ((MEA) — short or extended) to ensure an appropriate level of security and reliability. The studies yielded the following results:

1. A method for ensuring confidentiality and integrity SI in ABS on hybrid crypto-code designs on unprofitable codes. The method is based on a modified crypto-code system to McEliece modified geometrical codes that are integrated (a mechanism) provides IS SI (safe time — $T_B > 200$ g., Resistance to cryptanalysis $L_{CD} < 10^{25} - 10^{35}$ group operations), transmission reliability SI in ABS ($R_{error} < 10^{-9}$), and reduce energy costs in their practical implementation in 10^{-12} times (encryption, decryption) by decreasing order of $GF(q)$. Implementation of the proposed methods can improve security SI in ABS
2. The method of two-factor authentication based on HCCDUC MNCCS McEliece and Niederreiter of MES that provides a level of stability OTP passwords during transmission channels of communication open and to keep the possibility of further use of two-factor authentication protocol based on SMS-messages. Despite the decrease in power Galois field to $GF(2^6)$ for MNCCS and $GF(2^4)$ for HCCDUC statistical characteristics of crypto-code constructions were at least no worse than traditional NCCS McEliece in $GF(2^{10})$. All cryptosystem tests were 100 %, and showed the best result in shortened HCCDUC MEC: 155 189 tests completed at 0.99, which is 82 % of the total number of tests. This traditional NCCS McEliece in $GF(2^{10})$ 149 tests showed at 0.99.

References in Chapter 3

1. A. A. Kuznetsov, S. P. Evseev, S. V. Kavun, O. G. Korol' Signaly i kody. Algebraicheskie metody sinteza. Monografiya. – Khar'kov, Ukraine: Ed. KhNEU, 2009.
2. A. A. Kuznetsov, S. P. Evseev, S. V. Kavun Zashchita informatsii i ekonomicheskaya bezopasnost' predpriyatiya. Monografiya. – Khar'kov, Ukraine: Ed. KhNEU, 2009.
3. C. P. Evseev, O. G. Korol' Issledovanie kollizionnykh svoystv kodov autentifikatsii soobshcheniy UMAC. Informatsionnye tekhnologii i sistemy v upravlenii, obrazovanii, nauke. Monografiya/edited by V. S. Ponomarenko. – Khar'kov, Ukraine: Tsifrovaya tipografiya, p. 25–38, 2013.
4. C. P. Evseev, A. Yu. Yokhov, A. G. Korol' Kheshirovaniya dannykh v informatsionnykh sistemakh. Monografiya. – Khar'kov, Ukraine: Izd. KhNEU, 2013.
5. S. P. Evseev, and T. A. Sverdlo Issledovanie ugroz metodov dvukhfaktornoy autentifikatsii. Informatsionnye tekhnologii i zashchita informatsii v informatsionno-kommunikatsionnykh sistemakh. Monografiya/edited by V. S. Ponomarenko. – Kharkov, Ukraine: Ed. Ltd. "Shchedra sadiba plus", p. 141–154, 2015.
6. S. Evseev, V. Abdulaev Algoritm monitoringa metoda dvukhfaktornoy autentifikatsii na osnove sistemy Passwindow//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, ed. 2/2 (74), p. 9–15, 2015 (Scopus).
7. S. Evseev, O. Korol', Kh. Rzaev, Z. Imanova Razrabotka modifitsirovannoy nesimmetrichnoy kripto-kodovoy sistemy Mak-Elisa na ukorochennykh ellipticheskikh kodakh//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, Vol. 4/9 (82), p. 18–26, 2016 (Scopus).
8. S. Yevseiev, H. Kots, and Y. Liekariev Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, ed. 6/4 (84), p. 11–23, 2016 (Scopus).
9. S. Yevseiev, O. Korol', and H. Kots Construction of hybrid security systems based on the crypto-code structures and flawed codes//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, Vol. 4/9 (88), p. 4–20, 2017 (Scopus).
10. S. Yevseiev, H. Kots, S. Minukhin, O. Korol', and A. Kholodkova The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, Vol. 5/9 (89), p. 19–35, 2017 (Scopus).

11. S. Evseev Analiz metodov postroeniya universal'nykh klassov klesh-funktsiy//Vestnik Gosudarstvennogo universiteta informatsionno-kommunikatsionnykh tekhnologiy, vol. 7 (№ 4), p. 337–345, 2009.
12. S. Evseev, B. Tomashevskiy Issledovanie teoretiko-kodovykh skhem dlya kompleksnogo obespecheniya bezopasnosti i dostovernosti dannykh v informatsionnykh sistemakh//Nauchnyy vestnik Chernovitskogo universiteta. Series: Komp'yuternye sistemy i komponenty, vol. 2, ed. 1, p. 6–14, 2011.
13. A. Kuznetsov, O. Korol', S. Evseev Issledovanie kollizionnykh svoystv kodov autentifikatsii soobshcheniy UMAC//Prikladnaya radioelektronika, vol. 11, № 2, p. 171–183, 2012.
14. S. Evseev, O. Korol', L. Parkhuts' Razrabotka modeli i metoda kaskadnogo formirovaniya MAS s ispol'zovaniem modulyarnykh preobrazovaniy//Zashchita informatsii, vol. 15, № 3, p. 186–196, 2013.
15. S. Evseev, O. Korol' Issledovanie metodov dvukhfaktornoy autentifikatsii//Sistemy obrabotki informatsii, № 2 (118), p. 81–87, 2014.
16. S. Yevseiev, T. Sverdlo, and O. Korol' Mécanismes intégrés de sécurité et de fiabilité des données dans les systèmes d'information basés sur la théorie des codes correcteurs d'erreurs//French Journal of Science and Education, № 2 (12), p. 358–368, 2014.
17. S. Evseev, and B. Tomashevskyy Two-factor authentication methods threats analysis//Radio Electronics, Computer Science, Control, VIP. 1 (32), p. 52–59, 2015.
18. S. Evseev, Kh. Rzaev, A. Tsyganenko Analiz programmnoy realizatsii pryamogo i obratnogo preobrazovaniya po metodu nedvoichnogo ravnovesnogo kodirovaniya//Bezopasnost' informatsii, vol. 22, № 2, p. 196–203, 2016.
19. S. Evseev Ispol'zovanie ushcherbnykh kodov v krypto-kodovykh sistemakh//Sistemy obrabotki informatsii, № 5 (151), p. 109–121, 2017.
20. S. Evseev, S. Ostapov, R. Korolev Using mini-versions for evaluation of the stability of block-symmetric ciphers//Bezopasnost' informatsii, vol. 23, № 2, p. 100–108, 2017.
21. S. Evseev, A. Androshchuk, V. Fedorchenko Postroenie sistem bezopasnosti informatsionno-telekommunikatsionnykh sistem na osnove kompleksnogo krypto-graficheskogo podkhoda//Sbornik nauchnykh trudov Nats. akademii Gos. prikor. sluzhby Ukrainy im. Bogdana Khmel'nitskogo. Series: voennye i tekhnicheskije nauki/edited by Alekseenko B. M., № 2 (72), p. 258–268, 2017.
22. S. Evseev, A. Korol' Issledovanie ugroz metodov dvukhfaktornoy autentifikatsii//Vestnik Natsional'nogo universiteta "Lvovskaya politehnika", № 806, p. 62–71, 2014.

23. S. Evseev, O. Korol' Metod kaskadnogo formirovaniya MAS-kodov na osnove modulyarnykh preobrazovaniy//Izvestiya Vysshikh tekhnicheskikh uchebnykh zavedeniy Azerbaydzhana, № 1 (89), p. 71–78, 2014.
24. S. Evseev, O. Misyura Kripto-kodovye sistemy s otkrytym klyuchom na algebraicheskikh kodakh, at "Securitatea informațională 2008", (ed. a 5-a jubiliară), Grigore Bilostecinic, p. 64–66, 2008.
25. S. Evseev, O. Korol', V. Kovtun Autentifikatsiya dannykh s ispol'zovaniem klyuchevykh kheshiruyushchikh funktsiy. II Mezhdunarodnaya nauchno-prakticheskaya konferentsiya "Problemy i perspektivy razvitiya IT-industrii". – Khar'kov, p. 215–216, 2010.
26. S. Evseev, O. Korol' Metod universal'nogo kheshirovaniya na osnove modulyarnykh preobrazovaniy. III Mezhdunarodnaya nauchno-prakticheskaya konferentsiya "Problemy i perspektivy razvitiya IT-industrii". – Khar'kov, p. 131–132, 2011.
27. S. Evseev, S. Golovashich, I. Vorontsov Issledovanie mekhanizmov dvustoronney autentifikatsii soobshcheniy s ispol'zovaniem plastikovykh kartochek PASSWINDOW. IV Mezhdunarodnaya nauchno-prakticheskaya konferentsiya "Problemy i perspektivy razvitiya IT-industrii". – Khar'kov, p. 221, 2012.
28. S. Evseev Issledovanie metodov dvukhfaktornoy autentifikatsii/S. Evseev. VII mezhdunarodnaya nauchno-prakticheskaya konferentsiya "Sovremennye problemy i dostizheniya v oblasti radiotekhniki, telekommunikatsiy i informatsionnykh tekhnologiy" – Zaporozh'e, p. 331–332, 2014.
29. S. Evseev, T. Sverdlo Issledovanie ugroz metodov dvukhfaktornoy autentifikatsii. VII Mezhdunarodnaya nauchno-prakticheskaya konferentsiya "Problemy i perspektivy razvitiya IT-industrii". – Khar'kov, p. 26, 2015.
30. S. Evseev, I. Beloded Kripto-kodovaya sistema na modifitsirovannykh kodakh. V Mezhdunarodnaya nauchno-tekhnicheskaya konferentsiya "Metody i sredstva kodirovaniya, zashchity i uplotneniya informatsii". – Vinnitsa, p. 47–50, 2016.
31. S. Evseev, I. Beloded Ispol'zovanie ubytochnykh kodov v gibridnykh kripto-kodovykh konstruktsiyakh. V mezhdunarodnaya nauchno-tekhnicheskaya konferentsiya "Problemy informatizatsii". – Cherkassy – Baku – Bel'sko-Byala – Poltava, p. 11, 2017.
32. R.J. McEliece A Public-Key CRYPTOSYSTEM Based on Algebraic Theory. DGN Progres Report 42–44, Jet Propulsi on Lab. Pasadena, CA. January – February, p. 114–116, 1978.
33. H. Niederreiter Knapsack-Type Cryptosystems and Algebraic Coding Theory. Probl. Control and Inform. Theory, V. 15, p. 19–34, 1986.

34. *R. Bleykhut* Teoriya i praktika kodov, kontroliruyushchikh oshibki. – M.: Mir, 1986.
35. *Dzh.-ml. Klark* Kodirovanie s ispravleniem oshibok v sistemakh tsifrovoy svyazi/edited by B. S. Tsybakova. – M.: Radio i svyaz', 1987.
36. *F. Dzh. Mak-Vil'yams, N. Dzh. A. Sloen* Teoriya kodov, ispravlyayushchikh oshibki. – M.: Svyaz', 1979.
37. *V. M. Muter* Osnovy pomekhoustoychivoy teleperedachi informatsii. – L.: Energoatomizdat. Leningrad, 1990.
38. *T. Kasami, N. Tokura, E. Iwadari, Ya. Inagaki* Teoriya kodirovaniya/edited by B. S. Tsybakova and S. I. Gel'fand. – M.: Mir, 1978.
39. *V. M. Sidel'nikov* Kriptografiya i teoriya kodirovaniya. Materialy konferentsii "Moskovskiy universitet i razvitie kriptografii v Rossii". – M.: MGU, p. 1–22, 2002.
40. *V. A. Mishchenko, Yu. V. Vilanskiy* Ushcherbnye tekсты i mnogokanal'naya kriptografiya. – Minsk: Entsiklopediks, 2007.
41. *V. A. Mishchenko, Yu. V. Vilanskiy, V. V. Lepin* Kriptograficheskiy algoritm MV 2. – Minsk, 2006.
42. *A. A. Bolotov and others* Algoritmicheskie osnovy ellipticheskoy kriptografii. – M.: MEI, 2000.
43. *G. L. Katsman, M. A. Tsfasman* Spektры algebrogeometricheskikh kodov// Problemy peredachi informatsii, v. 23, № 4, p. 19–34, 1987.
44. *I. R. Shafarevich* Osnovy algebraicheskoy geometrii. – M.: Nauka, 1972.
45. *V. D. Goppa* Kody na algebraicheskikh krivyykh. Dokl. AN SSSR, v. 259, № 6, p. 1289–1290, 1981.
46. *K. Shannon* Raboty po teorii informatsii i kibernetike. – M.: IL, 1963.
47. *A. Rukhin, J. Soto* A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800–22, 2000.
48. Programmnoe sredstvo kriptograficheskoy zashchity informatsii "Grifon-B". URL: <http://www.banksoft.com.ua/index.php?id=28>.
49. Programmnoe sredstvo "Biblioteka funktsiy kriptograficheskoy zashchity informatsii "Grifon-L". URL: <http://www.banksoft.com.ua/index.php?id=27>. Accessed on: 1.12.2017.
50. Reshenie po mnogofaktornoy autentifikatsii 2FA One. URL: <https://habr.ru/company/1cloud/blog/277901/>. Accessed on: 1.12.2017.
51. Digital Authentication Guideline. URL: <http://www.3dnews.ru/936742?from=related-grid&from-source=940476/>. Accessed on: 1.12.2017.
52. Distantcionnoe bankovskoe obsluzhivanie klientov: sposoby zashchity tranzaktsiy. URL: http://www.prostobiz.ua/rko/stati/distantcionnoe_

- bankovskoe_obslyuzhivanie_klientov_sposoby_zaschity_tranzaktsiy. Accessed on: 1.12.2017.
53. Nastroyka dvukhfaktornoy autentifikatsii. URL: <http://support.citrix.com/proddocs/topic/web-interface-impington/nl/ru/wi-configure-two-factor-authentication-grandsden.html?locale=ru>. Accessed on: 1.12.2017.
54. Human In The Mobile Attacks Highlight Weaknesses In Out-Of-Band Authentication/Information week, 2010. URL: <http://www.darkreading.com/risk/man-in-the-mobile-attacks-highlight-weaknesses-in-out-of-band-authentication/d/d-id/1134495>. Accessed on: 1.12.2017.
55. C. Zeitz Security issues of Internet-based biometric authentication systems: risks of Man-in-the-Middle and BioPhishing on the example of BioWebAuth/C. Zeitz, T. Scheidat, J. Dittmann, C. Vielhauer, E. G. Agulla, E. O. Muras, C. G. Mateo, J. L. Alba Castro//Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, 2008. – 12 p. URL: <http://spie.org/Publications/Proceedings/Paper/10.1117/12.767632>, doi:10.1117/12.767632.
56. E. Barkan, E. Biham, N. Keller Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication//Journal of Cryptology, vol. 21, Issue 3, p. 392–429, 2008. doi: 10.1007/s00145-007-9001-y.
57. B. Winterford \$45k stolen in phone porting scam/B. Winterford//IT-news, 2011. URL: <http://www.itnews.com.au/News/282310,45k-stolen-in-phone-porting-scam.aspx/0>. Accessed on: 1.12.2017.
58. M. J. Schwartz, M. J. Zeus Banking Trojan Hits Android Phones/M. J. Schwartz//Information week, 2011. URL: <http://www.informationweek.com/mobile/zeus-banking-trojan-hits-android-phones/d/d-id/1098909>. Accessed on: 1.12.2017.
59. Trojan Writers Target UK Banks with Botnets/TechWorld, 2010. URL: <http://news.techworld.com/security/3228941/trojan-writers-target-uk-banks-with-botnets>. Accessed on: 1.12.2017.
60. R. V. Grishchuk, Yu. G. Danik Osnovi kibernetichnoi bezpeki. Monografiya/edited by Yu. G. Dannika. – Zhitomir: ZHNAEU, 2016.
61. Kiberbezopasnost' 2016–2017: Ot itogov k prognozam. URL: <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2016-2017-rus.pdf>. Accessed on: 1.12.2017.
62. Rise of IoT Botnets Showcases Cybercriminals' Ability to Find New Avenues of Attack. URL: http://storage.pardot.com/44731/127332/Cybercrime_Trends_Report_2016_Year_in_Review_1_.pdf. Accessed on: 1.12.2017.
63. Issledovanie HP: Sredniy godovoy ushcherb ot kiberatak vyros do 15 mln doll. na organizatsiyu. URL: <http://www.connect-wit.ru/issledovanie-hp->

- crednij-godovoj-ushherb-ot-kiberatak-vyros-do-15-mln-doll-na-organi-zatsiyu.html. Accessed on: 1.12.2017.
64. CISCO: Kiberataki na industrial'nye sistemy usilivayutsya, a doverie k imeyushchimsya sistemam zashchity padaet. URL: https://www.cisco.com/c/ru_ru/about/press/press-releases/2016/01-21a.html. Accessed on: 1.12.2017.
65. Банк данных угроз безопасности информации. URL: <http://bdu.fstec.ru/vul>. Accessed on: 1.12.2017.
66. *M. Slyman* An evaluation of hypothetical attacks against the PassWindow authentication method/M. Slyman, S. O'Neil, G.H. Nicolae, B. van der Merwe The PassWindow method, 2009. URL: http://www.passwindow.com/evaluation_of_hypothetical_attacks_againag_passwindo.pdf. Accessed on: 1.12.2017.
67. SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash. URL: https://csrc.nist.gov/publications/.../800-185/sp800_185_draft.pdf. Accessed on: 1.12.2017.
68. Guide for Cybersecurity Event Recovery. URL: <https://nvlpubs.nist.gov/nistpubs/.../NIST.SP.800-184.pdf>. Accessed on: 1.12.2017.
69. Security requirements for cryptographic modules. URL: <https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>. Accessed on: 1.12.2017.
70. GuidetoLTESecurity. URL: https://csrc.nist.gov/publications/drafts/800-187/sp800_187_draft.pdf. Accessed on: 1.12.2017.
71. Annex A: Approved Security Functions for FIPS PUB 140-2. URL: <https://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf>. Accessed on: 1.12.2017.
72. Annex B: Approved Protection Profiles for FIPS PUB 140-2. URL: <https://csrc.nist.gov/publications/fips/fips140-2/fips1402annexb.pdf>. Accessed on: 1.12.2017.
73. Annex C: Approved Random Number Generators for FIPS PUB 140-2. URL: <https://csrc.nist.gov/publications/fips/fips140-2/fips1402annexc.pdf>. Accessed on: 1.12.2017.
74. *L. Shapiro* Autentifikatsiya i odnorazovye paroli. Chast' 2. Vnedrenie OTP dlya autentifikatsii v AD. URL: <https://elibrary.ru/item.asp?id=20464277>. Accessed on: 1.12.2017.
75. *S. Evseev* Sinergeticheskaya model' otsenki bezopasnosti bankovskoy informatsii//Informatsionnaya bezopasnost', № 4 (24), p. 104-118, 2016.

CHAPTER 4. Development effectiveness evaluation approach to investment banking in information security in automated banking system

4.1 Development of evaluation method investment information security of banking information in terms of simultaneous action of threats to information security, cyber security and banking information

4.1.1 Development of composite indicator of investment in the system of banking information security in automated banking systems

Development OPS closely associated with the intensive development of information technologies as the Internet computer system and its information resources.

OPS related to critical infrastructure, which are crucial to public order, economic stability and national security states, it concerns the protection of national security, and so is the responsibility of the State [1, 16]. Information technology ABS is an integral part of business processes OPS in which information protection system (GIS) based on TZZI is used to ensure continuous and safe handling and BIn circulation.

Taking the decision to finance the creation and maintenance of all life stages of the GIS OPS seeking to significantly reduce material losses in the course of business, the cost of providing the IB BIn in ABS make up 30 % of all spending on information systems (IS) [2, 3, 4, 5, 6, 7, 18]. However, only 10 % of companies implement effective investment in information security, 40 % — are exposed to risks of large quantities IB.

Thus, the problem of effective investment in ABS IB BIn with the rapid increase in the number of hybrid attacks on infrastructure ABS is not solved. This is confirmed by analysis of published works and existing approaches [9, 12, 13, 14, 18].

One of the main issues is to assess the efficacy OPS taking measures to ensure the security of all components; IB, CB, BI information assets BIn in ABS for maximum profit. Evaluation of effectiveness of investment in information security is currently a topical issue, because for evaluating investments in IT security company (OPS) should correlate the cost of IP and obtained benefits from the use TZZI in terms of financial and organizational perspectives [3].

Analysis of recent research [4, 5, 6, 7, 9, 12, 14, 15, 18] Showed that the market conditions any undertaking OPS focused on supporting competitiveness.

Continuous circulation of information assets BIn in ABS, the link between information resources BIn, effective functioning of the ABS in which they are processed, the final impact on the financial performance of commercial banks in Ukraine.

It is believed that the cost of information security (IS) OPS effective if they meet the requirements of government regulations and standards, the NBU and the IB commercial or state bank concept.

This understanding stems from the fact that for an objective assessment of economic benefit IB no universal method. The lack of reasonable and generally accepted methods for assessing investment in the security BIn often creates a situation of alleged contradictions between the results obtained in implementing the ABS TZZI OPS objectives and optimize costs, limit investment opportunities OPS.

In economic benefit usually means exceeding cost estimates outcomes relevant measures of total costs of their resources for the billing period [2, 7, 8, 18].

The complexity of evaluating the effectiveness of security measures in the BIn ABS OPS is caused by a number of circumstances. According to the theory evaluating the effectiveness of the quality of any object, including GIS, appears only in the course of its intended use (operation target) because the objective is to assess the efficacy of [9, 12, 13]. The analysis methods for assessing the effectiveness of investments showed [2, 3, 4, 5, 6, 7, 8, 9, 12, 13, 18] That are conventionally divided into three groups: financial (traditional quantitative) and qualitative (heuristic) and uncertain nature. General classification methods for evaluating investments provided Fig. 4.1.

To assess the economic component of the efficiency of IT projects in the world the most commonly used basic indicators of financial groups: the rate of return on investment (ROI), net present value (NPV), internal rate of return (IRR), payback period (Payback Period), the economic attractiveness (EVA), balanced Scorecard (BSC), total cost of ownership (TCO), etc.

However, when trying to estimate the net profit from the project with IB having significant difficulties because the methods originally designed for the analysis of financial investment instruments, taking into account mainly the direct costs and their direct effects and simply do not consider their mathematical models are important non-financial parameters and effects of the project IB. This group does not allow methods to adequately assess the real economic impact of the project complex information security (CISS) [3, 6, 12, 13, 17, 18].

Cost method evaluation (see Fig. 4.1) can be used only in dynamics. The absence of statistics because of privacy BIn does not allow investors to conduct a reasonable calculation of risks ABS.

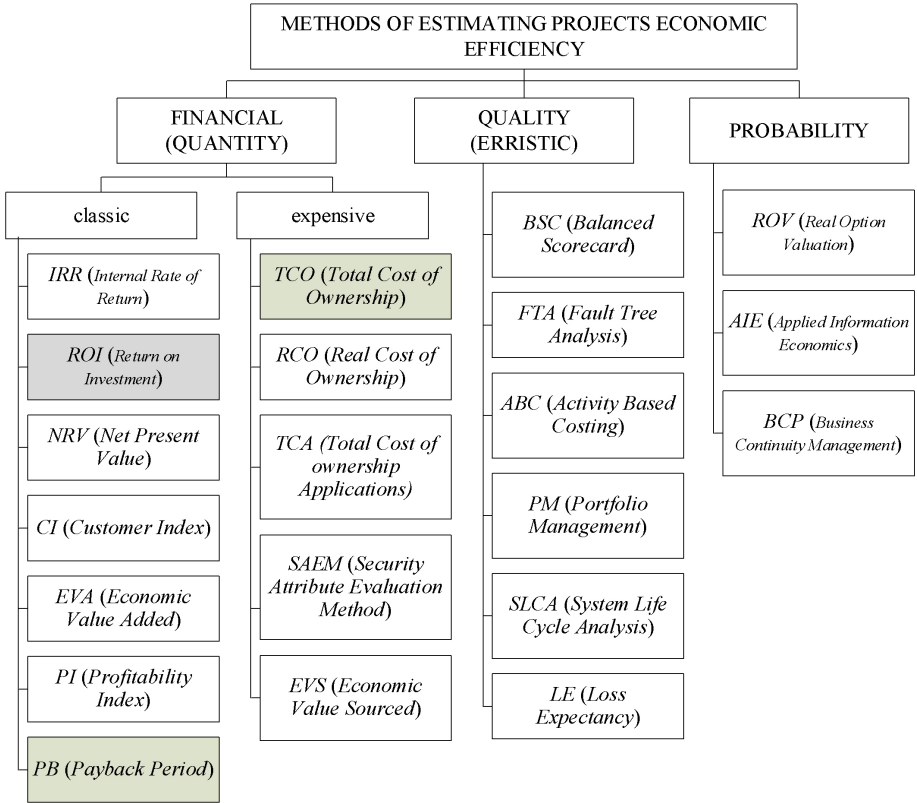


Fig. 4.1. Classification of methods to assess the economic efficiency of projects

This group of methods involves comparing the estimated project from already realized, this method actually can not find wide application in a highly competitive environment and the basis of existing companies in OPS privacy mode. Moreover, this analysis by comparing the project CISS — according disclose its composition — with other projects OPS (competitors) and third parties paradoxical and contrary to the main aim of the project [5, 14, 16, 18].

Group heuristic methods offers a comprehensive approach to assessment, but has limitations when evaluating projects CISS OPS. Thus, the method of Balanced Scorecard BSC (see Fig. 4.1) aims to develop management strategies based strategy maps based on grouping (comBIned) goals and metrics categories: finance, customers, processes, development, and so on. However, the use of the method does not introduce a strategic plan for OPS and does not require the rejection of traditional planning tools and control [7]. FTA method is based on two related assumptions about what components of

randomly destroyed in accordance with known probabilities of destruction, and the lowest level of the tree component failure independent of each other. The main disadvantages of the method are: uncertainty probabilities of basic events affecting the assessment of the likelihood of the final event; in some cases the events are unrelated, and sometimes difficult to determine whether we include all important ways to the end of [4]. Methods LE, PM, SLCA based on a comparison of losses from violations of security policy that can confront OPS and OPS investment in safety. Methods based on the analysis of expert groups OPS on which models are built “as is” and “how to”. The results of the expert group are largely subjective and do not give an objective assessment of the risks contained. These deficiencies characteristic of the group of empirical assessment methods.

Group probabilistic estimation methods (see Fig. 4.1) provides early implementation of specific management systems/quality management system (QMS) in the company OPS requires a significant investment of financial, human and time resources, aims not only to assess individual projects as the overall management of the company OPS and fit only for expensive long-term projects [5].

In addition, the methods do not consider important — BIn in ABS circulates in terms of simultaneous action on the system of information security threats, cyber-security and safety information. Only an approach that takes into account the hybrid threat (of synergies) for components of safety: IB, CB, BI BIn in ABS allows to obtain full and adequate assessment of the level of investment in information security BIn in ABS, which significantly affect the value of investments in the safety of the banking sector and opens the way to make informed management decisions on security.

Thus, the analysis methods of assessments of the effectiveness of investments in IB showed that the formation of an objective assessment of the efficiency of investment in the security BIn in ABS very laborious process, and usually evaluation of security measures in OPS reduced to finding categories:

- ROI, “Return on Investment”, investment rate of return;
- TCO, “Total Cost of Ownership”, total cost of ownership;
- PB, “Payback Period” payback.

To assess the costs of security BIn to use the OPS approach proposed in [3, 12, 13]. The specificity of the approach proposed is based on a mathematical model of synergetic threat assessment and improved model of the offender based on a synergistic approach improved classifier threats ABS [10, 11] And reduced to the calculation of a security risk BIn in ABS in terms of simultaneous action on the system of information security threats, cyber-security and safety information. This approach allows us to evaluate the continuity of the

functioning of business processes (processes information) and the ABS coefficient of internal rate of return on investment.

Presentation safety BIn as an information process, not a product, makes it possible to interpret the security of information assets as a multi risk management violations of safety OPS. As a result, risk management can achieve balance information risks for the activities of OPS, reducing the potential threat of hybrid components for security, IB, CB, BI aimed at computing facilities that process information resources. The results of the balance of risk information assets BIn selection is an effective method of control that allows to pinpoint BIn security settings and get the best return on investment for the construction CISS in ABS [13].

The formal description of the model estimates of investments in security BIn OPS, subject to necessary counter threats to hybrid BIn in ABS can imagine [3, 10, 11, 12, 13, 14, 19]:

$$W_{ABS}^{effinv} = \left\{ I_{O^{ABS}}, \Delta^{ABS}, \{DF^{ABS}\}, rang^{ABS}, \{SZ^{ABS}\}, d^{ABS}, D^{ABS} \right. \\ \left. ROI^{ABS}, NPV^{ABS}, ROSI^{ABS}, r^{ABS}, CV^{ABS}, OU^{ABS} \right\}, \quad (4.1)$$

where: $I_{O^{ABS}}$ — the value of information assets;

Δ^{ABS} — a sign of cost-effectiveness;

$\{DF^{ABS}\}$ — set of sources of threats to the safety components: IB, CB,

BI BIn ABS [10];

$rang^{ABS}$ — Rank development process TZZI (GIS);

$\{SZ^{ABS}\}$ — set TZZI (GIS) [10];

d^{ABS} — present value of cash flow;

ROI^{ABS} — rate of return on investment;

NPV^{ABS} — the net present value;

$ROSI^{ABS}$ — ROI TZZI (GIS);

r^{ABS} — factor of profitability in the security BIn;

CV^{ABS} — the degree of risk per unit of average income;

D^{ABS} — income from the use TZZI (GIS);

OU^{ABS} — estimate of income from the use TZZI (GIS).

The importance of information assets BIn evaluate the expression:

$$I_{O^{ABS}} = \frac{E_{BIn}^{ABS}}{Y_{BIn}^{ABS}}, \quad (4.2)$$

where: E_{BIn}^{ABS} — the cost of information resources (IR BIn) BIn;

Y_{BIn}^{ABS} — capital invested in the operation of the IP BIn.

Signs of cost effectiveness Δ^{ABS} evaluate the expression:

$$\Delta^{ABS} = \frac{e}{b}, \quad (4.3)$$

where: e — expected economic effect;

b — TZZI(GIS) development costs.

If a commercial bank OPS weighs feasibility of a project, in the simplest case, it can calculate the provided net cost of NPV^{ABS} income and expenses that will project and compare them. In other words, the return on investment should exceed the costs and profitability OPS establish their own [3].

$$ROI^{ABS} = NPV_{inv}^{ABS} - NPV_{zt}^{ABS}, \quad (4.4)$$

where: NPV_{inv}^{ABS} — income from investments in TZZI(GIS) ABS;

NPV_{zt}^{ABS} — costs TZZI(GIS) ABS;

ROI^{ABS} — return on investment in TZZI(GIS) ABS.

The same approach applies to assess the feasibility of investing in the security BIn in ABS. The main difference — investments in security BIn in ABS is not profitable, but only hypothetically prevent costs. Thus, TSZI OPS ABS should prevent costs more than the money spent on their development and implementation in TZZI(GIS) ABS, which will talk about ROI TSZI ($ROSI^{ABS}$) [3, 15]:

$$ROSI^{ABS} = NPV_{zbtzsi}^{ABS} - NPV_{zvtszi}^{ABS}, \quad (4.5)$$

where: NPV_{zbtzsi}^{ABS} — the cost of removal without compromising security embedded TZZI (GIS);

NPV_{zvtszi}^{ABS} — the cost of removal of compromised security with embedded TZZI (GIS).

This net present value NPV^{ABS} calculated by the expression:

$$NPV_{zbtzsi}^{ABS} = \sum_{i=1}^N \frac{ALE_i}{(1+r)^i}, \quad NPV_{zvtszi}^{ABS} = C_{sz} + \sum_{i=1}^N \frac{ALE_i}{(1+r)^i}, \quad (4.6)$$

where: N — number of intervals investments;

ALE_i — expected losses in the i -th period;

r — discount rate;

C_{sz} — cost remedies.

For improving synergies in the security BIn ABS hybrid in terms of countering threats to security components: IB, CB, BI integration of threats should be considered:

$$DF^{ABS} = \{V^{NS}\} \cup \{V^{AS}\}, \quad (4.7)$$

where $\{V^{AS}\} = \{V^{ASBI}\} \cap \{V^{ASIB}\} \cap \{V^{ASKBr}\}$, in which V^{NS} — class natural sources of threats $V^{AS} = \{V^{ASIB}, V^{ASBI}, V^{ASKBr}\}$ — class anthropogenic threats,

where V^{ASIB} — set of information security threats, V^{ASBI} — set of information security threats, V^{ASKB} — set of cyber security threats. Each element of the plurality of threats $DF_i \in \{DF^{ABS}\}$ Can be presented as a vector value $DF_i(p, u, risk)$, where p — the probability of threats, u — potential loss, $risk$ — the risk is expressed in a qualitative manner and takes one of two states $T_{risk} = \{\text{valid, invalid}\} = \{\alpha_{r1}, \alpha_{r2}\}$.

When BIn risk calculation method applicable. Annual loss expectancy — ALE, is the expected loss in each period of evaluation:

$$ALE^{ABS} = \sum_{i=1}^n I(O_{DF}^{ABS}) F_i, \quad (4.8)$$

where: $\{O_{DF}^{ABS}\}$ — set of threats;

$I(O_{DF}^{ABS})$ — cost implications of the threat;

ALE^{ABS} — the expected loss on sale;

F_i — Frequency (feature) of threats.

Development costs TZZI (GIS) ABS OPS are determined by rank. Evaluation rank TZZI development (GIS) ABS OPS $rang^{ABS}$ carried by the expression:

$$rang^{ABS} = \frac{SUM \times p}{s_{OPZ}^{ABS}}, \quad (4.9)$$

where: SUM — expected profit from the introduction TZZI (GIS) in ABS OPS;

p — probability of success using TZZI (GIS);

s_{OPZ}^{ABS} — costs of developing, implementing and maintaining the level of protection TZZI (GIS).

Present value of cash flow d^{ABS} estimated by the expression:

$$d^{ABS} = D_r + ROI^{ABS}, \quad (4.10)$$

where: D_r — discount rate;

ROI^{ABS} — return on investment in TZZI (GIS) ABS.

ROI factor B BIn r^{ABS} calculated by the expression:

$$r^{ABS} = \sum_{t=1}^T \frac{CF_t}{(1 + ROSI^{ABS})^t}, \quad (4.11)$$

where: t — the beginning of the time period;

CF_t — cash flow in period t ;

$ROSI^{ABS}$ — revenue from the project;

T — the end of the time period.

Assessment of degree of risk per unit of average income CV^{ABS} obtain using the expression:

$$CV^{ABS} = \frac{\sigma(E)}{\mu(E)}, \quad (4.12)$$

where: $\sigma(E)$ — standard deviation costs of the TZZI(GIS) OPS;

$\mu(E)$ — expectation for realization TZZI(GIS) OPS.

Income D^{ABS} the use TZZI(GIS) evaluate the expression:

$$D^{ABS} = Cost_1 P_D - Cost_2 (1 - P_D), \quad (4.13)$$

where P_D — the probability of income;

$(1 - P_D)$ — the probability of losses;

$Cost_1, Cost_2$ — unit cost information assets.

The proposed model is based on an assessment of investment in the security BIn OPS hybridity based on threats BIn in ABS and discounting of future cash receipts and expenses. Thus, this model takes into account the change in the security BIn investment OPS over time.

Characteristic changes in investment flow is the $l(t)$ intensity the number of average changes in flow per time unit [13]. The intensity intervals to evaluate $\Delta t_{[i-q]}$ between changes that have occurred in the stream using the expression [13, 15, 19]:

$$\Delta t_{[i-q]}(t) = \frac{K}{l(t)}, \quad (4.14)$$

where: K — the total number of changes of investments;

$l(t)$ — the intensity of the investment flow;

$i, q \in [1; n]$ — numbers change; $i \geq q$.

Changes in the investment process safety BIn OPS described as a finite automaton HABS, which describes the state of expression [13, 15, 19]:

$$H^{ABS} = \langle S_j^I, value, \Pi, S_0^I \rangle, \quad (4.15)$$

where: S_j^I — final state investments;

$value$ — changes in value of investments;

Π — investment function transitions from state k to state j ;

S_0^I — initial state investment.

Function Conversion investments Π from state k to state j is estimated by the expression:

$$\Pi = S_k^I \times value \rightarrow S_{k+1}^I \times value \rightarrow \dots \rightarrow S_j^I. \quad (4.16)$$

Assessment of potential losses U^{ABS} get information assets from the expression:

$$U^{ABS} = p_{rj} u_j, \quad (4.17)$$

where: p_{rj} — probability of realization of at least one threat j -th asset;
 u_j — j -th value of the asset.

Calculation of the probability of at least one threat for each asset is performed by the expression:

$$p_{rj} = 1 - \prod_{i=1}^m (1 - pr_{ij}). \quad (4.18)$$

Thus, estimates of total expected loss OU^{ABS} consists of potential losses and is determined by the expression:

$$OU^{ABS} = \sum_{j=1}^n U^{ABS}. \quad (4.19)$$

The estimations allow for the synergy and hybridity threats to safety components, IB, CB, BI BIn in ABS to provide qualitative and quantitative indicators of investment in the security BIn: ROI^{ABS} (rate of return on investment), NPV^{ABS} (net present value), $ROSI^{ABS}$ (ROI TZZI(GIS)). This approach allows fast and timely to assess the profitability of investing in the security BIn in ABS, which enhances the safety of ABS in general.

To ensure investment optimization process based on peer review integral parameters defined criteria for evaluating the effectiveness of investment in the security BIn OPS.

Each parameter is assigned weight classes rule Fishburne [14]. Based on the fact that change is subject to criteria weighting coefficients decreasing progressively. In this first criterion ($i = 1$), is the first in a strictly ordered by importance criteria ranked number $i = 1, 2, \dots, n$, is the most important and has the greatest weight. This rule is given by the expression:

$$w_i = \frac{2(N - n + 1)}{N(N + 1)}, \quad (4.20)$$

where: w_i — weight Fishburne criteria for evaluating the effectiveness of investment in the security BIn OPS;

N — total number of parameters integral criterion for evaluating the effectiveness of investment in the security BIn OPS;

n — serial number parameter;

i — the number of parameters in the integrated evaluation criteria.

According to the formula Fishburne have:

$$w_1 = \frac{2 \times N}{N(N+1)}, w_N = \frac{2}{N(N+1)}, \gamma = \frac{w_1}{w_N} = N, \quad (4.21)$$

where γ — the multiplicity of weighting coefficients differences from each other.

Thus, forming a system of weighting coefficients Fishburne W_F^{ABS} , the terms:

$$w_i \in [0;1], W_F^{ABS} = \sum_{i=1}^N w_i, \quad (4.22)$$

where $i \in [1;N]$.

As an optimization measures in [12, 13, 15, 19] Proposed to use the total cost estimate of costs to eliminate the impact of threats and other causes disabling TZZI and total payments financing.

Estimated total value of expenses M^{ABS} eliminate the consequences of threats and other causes disabling TZZI carried by the expression:

$$M^{ABS} = \sum_{i=1}^m C_i, \quad (4.23)$$

where: C_i — the cost of the i -th degree;

m — the total number of steps taken.

Estimated total payments c_i funding sources formed by the formula:

$$c_i = \sum_{j=1}^n A_{i,j}, \quad (4.24)$$

where: c_i — total payments j -th source of funding;

$A_{i,j}$ — payment of the j -th source of funding;

$i, j = 1, \dots, n; n$ — number of funding sources.

The proposed model of efficiency investments in the security BIn OPS allows for efficiency investments by minimizing the cost of security BIn in ABS OPS in terms of countering threats to security components: IB, CB, BI, their integration of hybridization and synergy.

Minimize security expenses BIn in ABS OPS conducted the optimization process that reflects the following expression:

$$\min(E_1^{ABS} b_1 + E_2^{ABS} b_2 + \dots + E_j^{ABS} b_n), \quad (4.25)$$

where: E_j^{ABS} — j -criteria optimization and, $j = 1, \dots, n; n$ — number of criteria;

b_n — a sign of the j -th use of funding sources:

$$b_n = \begin{cases} 1, & \text{the source of use is used;} \\ 0, & \text{the source of use is not used.} \end{cases} \quad (4.26)$$

Within the framework of proposed model of efficiency investments in the security BIn ABS OPS evaluated the following parameters — the total value of the cost of liquidation of consequences of threats or other causes disabling information security systems, and total payment funding sources in order to determine acceptable levels of risks of IB BIn OPS in ABS. This ensures minimization of damage and the cost of security BIn in ABS OPS is effective because profits from implementation of GIS over invested capital [13, 15, 19].

Summarizing the parameters used in the framework of the proposed model, we define the integral criterion of efficiency of investment in the security BIn OPS using the expression:

$$W_{ABS}^{effinv} = \sum_{i=1}^N w_i M^{ABS} \quad (4.27)$$

Thus, the model of efficiency investments in the security BIn in ABS OPS can be in different states SABS, which can be described as the following sets:

$$S^{ABS} = \{S_1^{ABS}, S_2^{ABS}, \dots, S_m^{ABS}\}, \quad (4.28)$$

where: S^{ABS} — the set of possible states of the model;

S_1^{ABS} — the initial state of the model;

S_m^{ABS} — the final state of the model.

Thus, the method of evaluating the effectiveness of investments in the banking information security in automated banking systems which is based on a composite index investing to optimize the cost of funds for the construction of a system of information security in terms of hybrid threats of information security cyber-security and safety information. The practical implementation of the method allow to assess key indicators of investment in IT security given BIn synergistic evaluation of threats IB, CB, BI.

To evaluate the functional efficiency of data exchange network ABS in the next section the proposed method of evaluation based on comprehensive evaluation indicator of quality of service objects automated banking system for the safety of bank information.

4.1.2 The development of methods of cryptosystems stability evaluation based on entropy method for assessing the randomness of the original sequence

For the comparative assessment of effectiveness (cryptographic strength) symmetric encryption algorithms typically use methods of linear and differential cryptanalysis, milestones and performance are considered in [23]. The analysis shows that the differential and linear codes require full analysis of experts, significant economic, computing and human costs. Proposed and

developed in [24, 25, 26, 27, 28, 29, 30, 31, 32, 33] New sustainability assessment methodology of block symmetric ciphers to differential attacks and linear cryptanalysis is based on the established fact that all modern block ciphers after several initial cycles encryption acquire properties of random permutations appropriate degree [28, 30].

The basis of the developed approach is the provision according to which more codes repeat their properties reduced models. In [25, 26, 27, 28, 29, 30, 31, 32, 33] Showed that larger version codes when used in reduced mode encryption (16-bit and 32-bit) data blocks repeat the laws of probability distribution XOR transitions tables, tables and landslides linear approximations inherent applicable laws of probability distribution of its reduced versions. The latter, in turn, after several initial cycles of encryption comes to the laws of probability distribution XOR transitions tables and tables displacement approximations of random permutations [28, 30].

Comparison of safety on algorithms of traditional cryptography, public key cryptography, hybrid cryptosystem possible on the basis of the composite indicator that takes into account cryptographic strength criteria, crypto-conversion performance, transparency of encryption for user allocation key sequences investments in IT security that does not allow without significant time and economic costs to determine their effectiveness. Fig. 4.2 shows the proposed ideology.

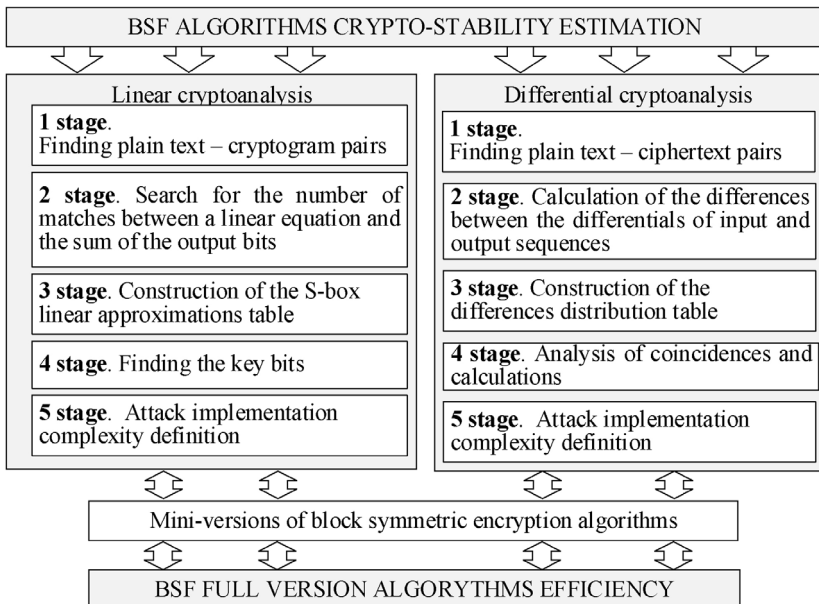


Fig. 4.2. Proposed ideology department BIT KNURE

Similar studies were carried out mini versions and foreign authors. Thus, in the works F.-X. Standaert and colleagues [34, 35] Studied the difference between theoretical and practical cipher resistance introduced by L. Knudsen [36]. And confirmed its significant dependence on the size of the block. Testing hypotheses equivalence keys on the mini-versions of AES showed that it should be done on a full-sized keys, for which the present code was designed.

The results obtained in [23] BSC simplified versions for evaluation of evidence-based models of full security codes to the differential attacks and linear cryptanalysis based on the increase of the login code confirms the possibility of their use. Adequacy assessment results BSC simplified model properties depends on the selection ratio, which determines the properties of their prototyping of complete ciphers.

Choice coefficient should be proportional to the maximum resource calculation means used for research. For each block symmetric cipher (among known iterative BSC) there is a definite number of cycles, after which the code takes on the properties of a random sequence. Further increasing the number of cycles does not affect the final properties of linear differential and encryption, enabling «reduce» the number of iterations and increase the speed crypto-conversion.

However, to maintain all the properties of a prototype simplified models of their adequacy prerequisite is the use of *mini-S-box*-along with key performance indicators nonlinear units substitutions (balance, nonlinearity, autocorrelation) at the level of full performance data ciphers.

Thus, to select a particular algorithm BSC enough to appreciate its original sequence in an accident.

To assess the stability of cryptographic encryption algorithms of different models proposed to use rapid analysis based on entropy methods used in statistical research package random variable NIST STS 822 [37]. The proposed enables rapid analysis without considerable computational, economic and human costs intuitively compare not only the stability of different encryption algorithms (cryptographic), but their software implementation.

The algorithm entropy method for assessing the reliability shown in Fig. 4.3.

Table 4.1 These results sustainability and efficiency of program implementation block and stream cipher varying complexity.

As used block ciphers DES, 3DES, GOST 28147–2009, Kalina-256, AES-256. To implement the stream cipher used generators pseudorandom sequence of two different types: the rule of «60» cellular automata in the classical form without modifications and cryptographic stable generator of crypto-library Secure-Random Java, which is positioned as suitable for cryptographic applications for assessing asymmetric cryptographic algorithm used RSA algorithm.

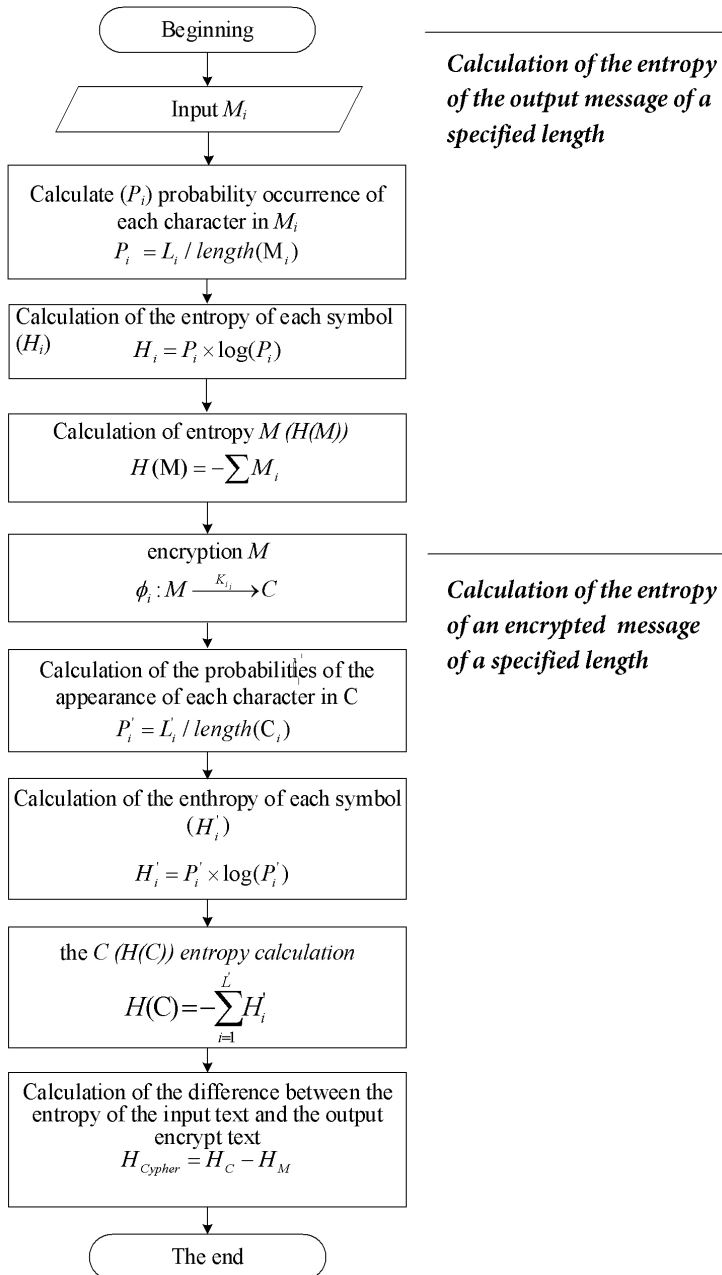


Fig. 4.3. The algorithm testing for resistance cryptosystem based on entropy evaluation method chance

Table 4.1. — The research results of stability algorithm rapid method

Number	Code	Entropy input text	Entropy crypto-grams	the difference between entropy	% Entropy that comes codes
1	Cellular automata rule “60”	0.5023775	0.6820179	0.1796404	35.7580505
2	Crypto-resistant generator with Java SecureRandom	0.5023767	0.7999982	0.2976215	59.2426958
3	DES	0.469276	0.812043	0.342767	73.0416642
4	3DES	0.469276	0.812043	0.342767	73.0416642
5	GOST 28147–2009	0.469276	0.811348	0.342072	72.8935637
6	Kalina-256	0.469276	0.954519	0.485243	103.4024753
7	AES-256	0.469276	0.95454	0.485264	103.4069503
8	RSA	0.469276	1	0.530724	113.094213214

Table 4.1 was calculated entropy input and ciphertext difference, and the percentage of entropy, which is attached to the entropy of the plaintext same codes. Analysis Table 4.1 makes it possible to estimate the contribution of the cipher in the final entropy encoded message. Because they are tested under identical conditions can judge their relative performance.

In this sense, it is worth noting AES-like cipher (SPN-system pidstano-vochno-adjustable schemes). Both of these encryption and Kalina-256 and AES-256 made the greatest contribution of over 103 % in the entropy of the plaintext. Thus, both have excellent dispersion cipher. Approximately the same figures showed symmetric block cipher (BSC) GOST 28147–2009 — 72.89 % compared to 73.04 % in DES/3DES. Perhaps this only confirms the findings of the maximum possible extent scattering characteristic architecture as BSC.

For comparison, the experiments using a stream cipher based on two different generators pseudorandom key sequence. Encryption is performed by adding the rule «module two.»

In the first case — a generator based on cellular automata (rule «60»). This is not crypto-resistant generator, the sequence has not tested NIST STS 822, and the second is positioned as crypto-resistant generator with SecureRandom Java crypto-library. In both cases, the values of entropy, far less than traditional BSC, which does not talk about quality encryption using them.

Asymmetric cryptography algorithm provides the highest rate investigated more than 113 % in the entropy of the plaintext to show its cryptographic strength evidence.

So are the results suggest that a simple rapid method based on entropy evaluation method chance cryptograms enables rapid assessment of quality codes used without the involvement of expert assessments of major economic, computing and human Trat. This rapid method is available to any user that has minimal knowledge of information theory. Moreover, this way you can evaluate the different implementations codes, which will choose the best (optimal) software implementation that is appropriate for the conditions and requirements of the user. For example, their computer experiments used two of the algorithm DES. One of them is shown in the table 4.1 at number 3, showed a growth of entropy after encryption 73.04 % of the input text, the other — 64.4 %.

Of course, for practical purposes, it makes sense to choose the first implementation, because, obviously, scattering characteristics it better. Thus, rapid analysis to evaluate quality of the classic (and others) encryption algorithms to select the optimal set of existing crypto-library market.

Consider the results in terms of maximum cryptographic protection. An indicator of this protection is entropy encoded executable listed in Table 4.2.

Table 4.2. — Estimated maximum cryptographic protection

Number	Code	Entropy input text	Entropy cryptograms	Probability crypto-protection, Pc
1	Cellular automata rule “60 “	0.469276	0.637079949	0.637079949
2	Crypto-resistant generator with Java SecureRandom	0.469276	0.747287753	0.747287753
3	DES	0.469276	0.812043	0.812043
4	3DES	0.469276	0.812043	0.812043
5	GOST 28147–2009	0.469276	0.811348	0.811348
6	Guelder rose	0.469276	0.954519	0.954519
7	AES-256	0.469276	0.95454	0.95454
8	RSA	0.469276	1.000	1.000
9	ideal cipher		1.000	1.000

We know that the best possible encryption enables TN «The perfect code» for Shannon, who as a result of encryption provides a random number [38]. This file will have maximum entropy, which is a BInary event is one. We assume that this encryption cipher will most encryption, and take it by 1. The probability of such protection codes equal to one. Naturally, imperfect codes do not give such a probability encryption.

Fig. 4.4 These results averaged entropy cryptograms different BSC meaningful plaintext length $M = 10^8$ bits, with an interval of $N = 5 \times 10^6$ bits.

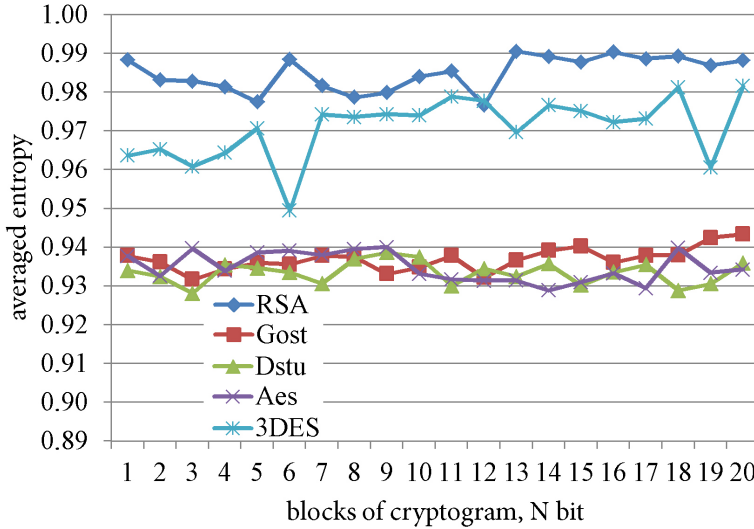


Fig. 4.4. The research results averaged entropy blocks cryptograms

Analysis Fig. 4.4 practically confirmed the possibility of using rapid method for choosing software security mechanisms based encryption algorithms.

Thus, the proposed method of evaluation of stability enables encryption algorithms to rank all probability studied ciphers through encryption. This figure can be used for different bases of complex security systems to protect various corporate networks, says its versatility.

4.2 Develop comprehensive measure of service quality evaluation objects automated banking system to ensure the safety of bank information

Remote Access Technologies and open Internet resources used in ABS OPS, can significantly extend the range of financial services through Internet banking and Web-resources of ABS. To ensure the safety components: IB, CB, BI BIn in ABS typically used certified cryptographic mechanisms NBU standardized procedures based on symmetric and asymmetric cryptography. The analysis standards in [39] Showed that the key principles of information security risk assessment is. In fact, the risk is an integrated assessment of how effectively the available means of protection able to withstand attacks information. Practice shows that today we can clearly distinguish two main groups of methods for assessing security risks [39, 40, 41].

The first group of methods allows you to set the level of risk by evaluating the extent to defined set of requirements for information security. The second group IB methods of risk assessment is based on determining probability of attacks and levels of damage. In this case, the risk value is calculated for each threat and, in general, is a product of the probability of threats to the size of potential losses from this threat. The value of damage is determined by the owner of the information and the probability of threats is calculated by the panel conducting the audit procedure.

These results basic methods of risk assessment used in OPS.

Table 4.3. — Methods risk

Evaluation method	Advantages	Shortcomings	Approaches
1	2	3	4
NIST	– Detailed description of the possible risks of information assets – For companies of different sizes	– long-term process analysis – Some features are not automated	Heuristic
FAIR	– Comprehensive analysis simulation models – High efficiency	– For large banks and enterprises	Probability
IT-Grundschutz	– The flexibility of the method allows to analyze any organization – Adjustable for new or existing assets	– Requires the theoretical knowledge of the process of risk analysis – The high cost of licenses	Heuristic
OC-TAVE	– Fast Implementation – Serving small and medium-sized enterprises	– Lack of automation – Do not take into account the specific banking	Heuristic
IRAM	– The relative ease of implementation – Easy to use managers of banks	– The high cost of licenses – Work only with existing inform. assets	Informative
EBIOS	– large number of users – Generate reports	– Only for commercial and government organizations	Informative

Continuous of the Table 4.3

1	2	3	4
RISK WATCH	– Ease of implementation and operation – Flexibility – High efficiency	– Risk analysis only on the software and technical level – The high cost of licenses	Informative
MEHARI	– Based on an analysis of formulas and parameters – Generates an optimal set of countermeasures – Public domain	– applicable to systems that are built only with ISO	Heuristic
MAG-ERIT	– Systematic analysis method – Quantifying – Flexibility	– The resulting data depends on the human factor	Heuristic
CRAMM	– Detailed definition of risk exposures – Efficiency	– The severity of understanding – The high cost of licenses – Work only with existing inform. assets	Probability
Methods NBU	– Detailed analysis of the resources of the banking system – Using a risk-based approach	– Based on a set of standards – Takes into account only the specificity Ukrainian banking system	Informative
Methods Korchenko	– Application Feature principle to describe the various classes CBA – Allows you to expand Feature space to describe new classes	– Do not allow to assess financial losses from sales of threat	Informative

The relationship between methods of intrusion detection and risk assessment methods are shown in Fig. 4.5.

The analysis table 4.3, 4.4 and Fig. 4.5 shows the methods and techniques do not allow for evaluation of functional performance indicators based on both technical and economic [42].

Table 4.4. — The results of research methods of risk assessment

Method	paraphernalia							
	Qualitative assessment	Quantifying	Comprehensive assessment	Country of Origin	The use of OPS	Software implementation	The effectiveness of counter-measures	Easy understanding
NIST	+			USA	+	+	–	–
FAIR			+	USA			+	+
EBIOS	+			France	+	+	+	–
MEHARI			+	France				
OCTAVE	+			USA	+			
IT-GRUNDSHULTZ	+			Germany			+	
IRAM	+			Europe				+/-
RISK WATCH		+		USA	+	+	+	+
FRAP	+			USA				
CRAMM			+	UK	+	+	+/-	+/-
MAGERIT	+	+		Spain	+	+		
Methods NBU	+			Ukraine	+		–	+
Methods Korchenko	+			Ukraine			+/-	+

Analysis of publications and standards of quality of service (Quality of Service, QoS) in IP networks [43, 44, 45, 46, 47, 48, 49, 50] Allowed to define the main technical parameters QoS — reliability and safety. Fig. 4.6 The results of fusion hybridity security threats components: IB, CB, BI BIn in ABS-based cyber and information on the impact of component indicators of quality of service QoS.

Thus, for the assessment of emergent properties of functional efficiency ABS must use complex quality based on key indicators of safety and reliability, which in turn provides a counteracting threats to BIn hybrid infrastructure and ABS.

The quality of these services is characterized by a set of basic consumer properties [51, 52, 53, 54, 55]: Security, usability, efficiency, safety and other properties specific to each service. In addition to these technical characteristics networks as performance, latency, scalability, degree of transparency for end users is extremely important features are integrated reliability, availability factor and the average time of unavailability per year. From performance reliability depends availability of services for users.

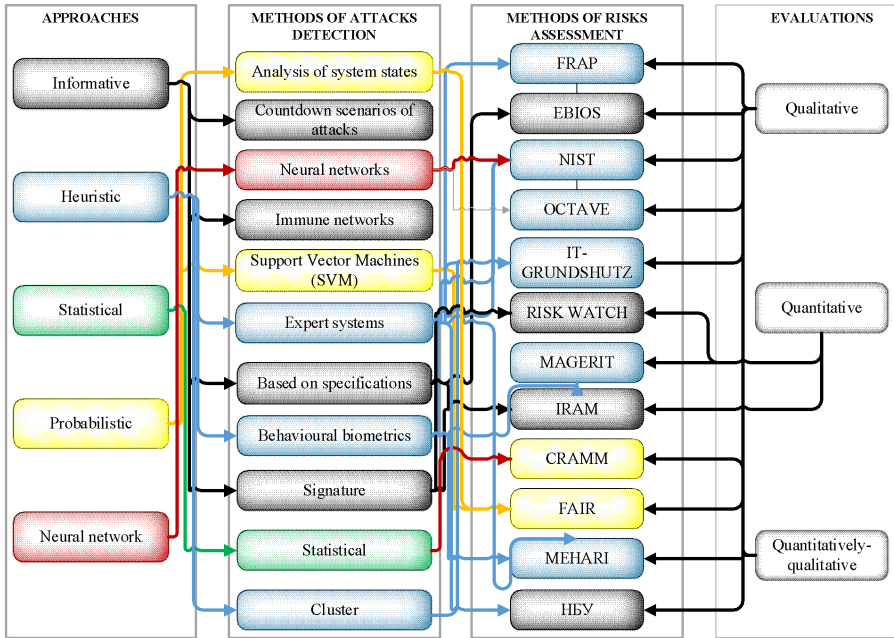


Fig. 4.5. The relationship between methods of intrusion detection and risk assessment methods

In addition, the reliability of the network and indirectly dependent network performance and latency as the cause of fires and failures on the network leading to the need for retransmission of data blocks, which ultimately leads to increased delays in the transmission and reducing the volumes of data transferred per unit time [53]. To assess the technical component of functional efficiency [42] Use the overall performance of data exchange, including velocity reliable and confidential data in a computer network ABS and allows you to compare the effectiveness of existing protocols, the exchange of data between two nodes seen in [51, 54, 55].

In reviewing the operation of IP-based networks used in ABS OPS, the overall performance of data exchange should include safety performance indicators and partial communication system — reliability and efficiency. The main criteria for evaluating the effectiveness of classified assumed the following [56, 57, 58, 59, 60, 61, 62, 63]:

1. Strong cryptography (secret number), which estimate the complexity of solving the problem of cryptanalysis best known method.
2. The amount of key data. Symmetric cryptosystem operates common to all users secret key. In this case, it requires secure distribution channels, which means that the key should not be too great not to have problems with its

distribution, and not so small that it was difficult to break the full bulkhead. If asymmetric cryptosystem is one of the keys can be public, its spread through open channels of communication.

3. The complexity of forward and backward cryptographic transformation (encryption/decryption of messages). These operations should be as simple, so they could easily be put into practice.

4. Reproduction number of errors. In some types of ciphers error in one letter made when encryption or transmission, resulting in a large number of errors in the decrypted text. Naturally, it is desirable to minimize error propagation.

5. Increase the message. In some types of secret message size increases as a result of the transaction encryption. This should minimize the undesirable effects.

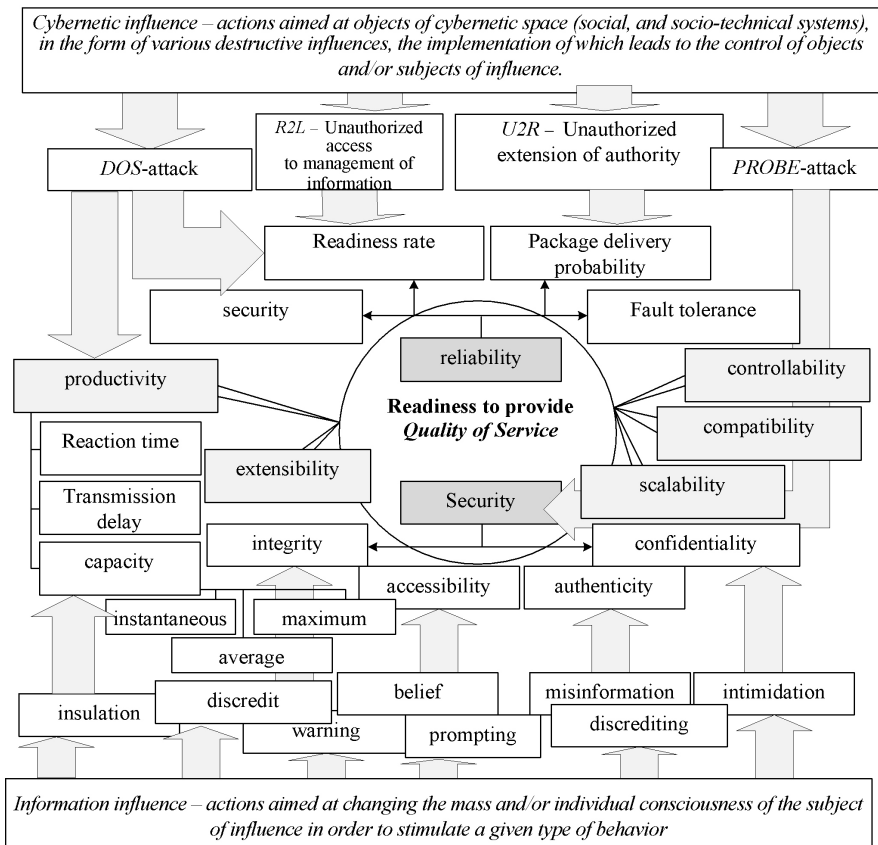


Fig. 4.6. Analysis of the hybridization of threats to security components (IB, KB, BI) of BIR based on cybernetic and informational influence on the components of QoS service quality indicators

To evaluate the efficiency of the components offered encryption algorithms use a fast and intuitive rapid method that enables ranking stability and efficiency of software encryption algorithms.

The stability of security in ABS on the possible actions of the attacker based on the theorem of multiplication probabilities of independent events expression:

$$B = P_A \times W_{synerg}^{IB,KB,BI} \quad (4.29)$$

where: B — stability security in ABS;

P_c — likelihood encryption TZZI in ABS;

$W_{synerg}^{IB,KB,BI}$ — the probability of realization of synergistic attack on BIn in

ABS on component safety: IB, KB, BI .

When property reliably understand the system, descriBing its ability to provide accurate reproduction of posts in receiving points [65]. Accuracy depends on the settings of the IP-network, degree of technical excellence and working conditions (type and status communications, meteorological parameters, the type and intensity of noise and organizational measures to the rules and operation of radio equipment) [54, 55, 65]. Quantitatively, the reliability of transmission can be determined: probability of erroneous reception of a single element (loss of authenticity):

$$P_0 = \lim_{n_{zag} \rightarrow \infty} \frac{n_{pom}}{n_{zag}}, \quad (4.30)$$

where: P_0 — probability of erroneous reception of a single element; bit error probability channel data;

n_{pom} — the number of individual elements mistaken;

n_{zag} — the total number of transmitted individual elements.

Probability of erroneous reception of the data packet:

$$P_{pom\ n} = \lim_{N_{zag} \rightarrow \infty} \frac{N_{pom}}{N_{zag}}, \quad (4.31)$$

where: $P_{pom\ n}$ — the probability of erroneous reception of the package;

N_{pom} — the number of code sequences erroneously received (packages);

N_{zag} — total transmitted code sequences (packages).

The probability of correctly receiving a single element $P_{0\ pr}$ and probability of correct reception of the package: $P_{pr\ n}$, and:

$$P_{0\ pr} + P_0 = 1; \quad P_{pr\ n} + P_{pom\ n} = 1, \quad (4.32)$$

where: $P_{0\ pr}$ — the probability of correctly receiving a single element;

$P_{pr\ n}$ — the probability of correctly receiving the package.

The probability of erroneous and the correct reception of a single element (P_0 and $P_{0\ pr}$) is actually a discrete communication channel characteristics, the

likelihood $P_{pom\ n}$ and $P_{pr\ n}$ are the characteristics of the computer network in general, as they are determined not only by the nature and intensity of noise in the channel called communications, modulation type and speed, but also a way to protect against errors in the system [54, 55, 65].

Delivery time information [54, 55, 65] — the time interval from the start of the message flow input data transmission of computer network prior to its delivery to the consignee data receiving part. When transmitting confidential information, in addition, the delivery includes encrypting the sender of data packets and a packet decoding receiver corresponding algorithm.

Analysis time encryption and decryption winners AES encryption algorithms and NESSIE [58, 59, 60, 61, 62, 63, 64] Shows that for asymmetric algorithms complexity of implementing cryptographic 3–5 orders of magnitude higher than that of similar block-symmetric ciphers, hybrid crypto-code design on unprofitable codes, providing speed crypto-conversion at BSC.

Thus, the IP-based network with autoreply (critical feedback) the delivery package is [51; 54]:

$$t_d = t_d' + \Delta t_d + t_{sh} + t_{rsh} \text{ — for symmetric encryption algorithms,}$$

$$t_d = t_d' + \Delta t_d + (t_{sh} + t_{rsh})^s \text{ — for asymmetric (hybrid on CCDUC) encryption algorithms,}$$

where: t_d — the delivery of the package;

t_d' — the delivery of the first package parcels;

Δt_d — a multiple repetition of information transfer due to deterioration of the quality of the channel;

t_{sh} — the encryption algorithm data packet;

t_{rsh} — a receiver decoding the data packet.

t_d — time message delivery to the specified address depends on many factors: the channel structure, reliability and network load, switching method, the presence and nature of disturbances that lead to errors and retransmissions. It is a random variable, characterized by a density distribution $f(t_d)$.

In channels with high error P_0 improve the reliability of results in increased delivery time t_d by reducing the number of repeat parcel package, and vice versa, reducing delivery time t_d by reducing the number of repeat parcels package leads to lower reliability [51; 54]. However, most real data channels are non-stationary, the probability of a single error in their time-varying widely from 10^{-9} to 10^{-12} [51, 54, 66, 67].

General requirements for the reliability of the information is to minimize the likelihood of erroneous reception P_{error} characters of the message or,

equivalently, to maximize the probability of correct reception $P_{\text{right receipt}}$. At the same time today the requirements for reliability of information increased significantly and, according to [44, 45] Acceptable probability of erroneous reception of message symbols $P_d < 10^{-7} - 10^{-9}$, depending on the category of information value, its priorities and equipment.

To calculate the comprehensive performance indicator data networks based on different technologies, you must use multivariate analysis, because in these cases accounted for entirely different factors: the cost of network deployment, speed data, probability and time of delivery of the package, and so on. Each of these indicators can be calculated separately by any method, but to calculate the integral index of common quantitative methods do not exist. Usually in such cases the models using multivariate analysis, the simplest of which was involved in this case.

To evaluate the integrated performance indicator has been developed supporting table that can provide ranges of changes necessary parameters and define them in arbitrary points. This simple method provides a fairly adequate evaluation results, and in addition, combine them with the results of precise calculations on certain specific parameters.

In the reference Tables 4.5–4.10 are parameters of data are taken into account in the integral index of the functional efficiency of the IP network.

Table 4.5. — The cost of network deployment

Points	Parameter description
1	Very high cost
2	The high cost
3	average price
4	Low cost
5	Very low cost

Table 4.6. — The data transfer rate

Points	Parameter description
1	Small (10Mb/s)
2	Average (100MB/s)
3	High (1GB/s)
4	Very high (10GB/s)
5	Extremely high (40 Gb/s)

Table 4.7. — The probability of packet delivery

Points	Parameter description
1	The small (> 0)
2	The average (0.95)
3	High (0.97546)
4	Very high (0.999999)

Table 4.8. — Package Delivery Time

Points	Parameter description
1	Very large (1875 c)
2	Big
3	Average
4	Small (0.006 s)
5	Very small (0.0003 s)

Table 4.9. — Delay package

Points	Parameter description
1	Great
2	The average
3	Small

Table 4.10. — Performance network

Points	Parameter description
1	Small
2	The average
3	High

Thus, based on multivariate analysis model can not describe completely different parameters that are otherwise analytically combine virtually impossible. For comparison data of existing technologies were selected as follows: packet switching by the standards of global computer networks (WAN): X.25; Frame Relay; Ethernet, Fast Ethernet; Gigabit, 10 Gb, 40 Gb Ethernet. Comparative characteristics of these technologies are shown in Tables 4.11–4.13.

Table 4.11. — Comparative characteristics of the Ethernet protocol

WAN technology	Cost	The data rate, Mb/s	Length package Bit	The probability of correct delivery package P_{prn}	The time to deliver the package, t_d, s
Ethernet	secondary	10	1518	0.95	0.006
Fast Ethernet	secondary	100	1518	0.95	0.006
Gigabit Ethernet	high	1000	1518	0.99999	0.006
10 GbE	high	10000	1518	0.99999	0.006
40 GbE	high	40000	1518	0.99999	0.006

Table 4.12. — Probability-time characteristics of WAN technologies

WAN technology	Cost	The data rate, Mb/s	Length package Bit	Probability P_{prn}	The time to deliver the package, t_d, s
X.25 (V.34)	secondary	10	1056	0.97546	1875
Frame Relay	secondary	100	12048	> 0	0.0003
Fast Ethernet	secondary	100	1518	0.95	0.006

Using data from the table. 4.5–4.13, get a table generalized efficacy data networks, where selected indicators are presented in standard scores.

Table 4.13. — Comparing Ethernet, packet switching and Frame Relay

Indexes	Fast Ethernet	Packet switching (X.25)	Frame Relay
Time Division Multiplexing	do not have	do not have	do not have
Statistical multiplexing	So	So	So
Separation ports	So	So	So
High performance	So	do not have	So
Delay	low	high	low

Table 4.14. — Generalized data networks efficiency

Technology	Cost	Speed	The probability of packet delivery	Delivery time	Delay package	Productivity	Consolidated Performance Index	The relative efficiency, %
X.25	3	1	3	1	1	1	9	0.25
Frame Relay	3	2	1	5	3	3	270	7.37
Ethernet	3	1	2	4	3	3	216	5.89
Fast Ethernet	3	2	2	4	3	3	432	11.79
Gigabit Ethernet	2	3	4	4	3	3	864	23.59
10 Gb Ethernet	2	4	4	4	3	3	1152	31.45
40 Gb Ethernet	1	5	4	4	3	3	720	19.66
Total:							3663	100

The results are shown in Table 4.13 displayed on Fig. 4.7, 4.8.

As seen from the table 4.14 and Fig. 4.7, 4.8, offered a simple approach provides a fairly adequate result. It is seen that the most effective on the totality of these indicators is 10 Gb Ethernet. Popular for commercial communications Fast Ethernet is not fully “charged” with growing traffic and 40 Gb Ethernet is quite expensive for the end user, which does not classify it as an optimal network infrastructure.

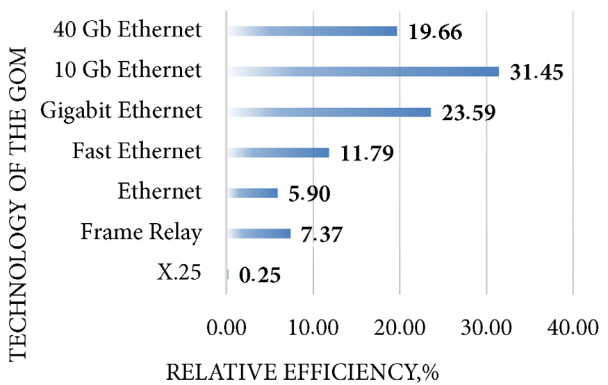
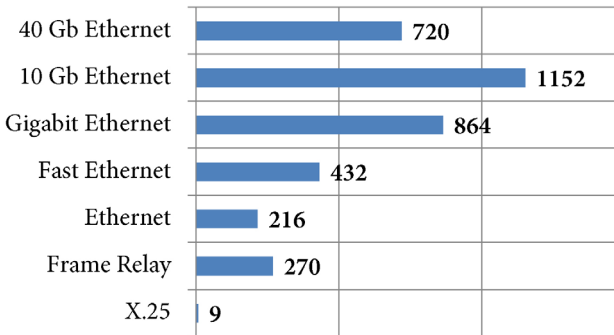


Fig. 4.7. Comprehensive performance indicator different technology networks

Fig. 4.8. Normalized indicator of the effectiveness of various technologies COP, W_{norm}

However, 10 Mb Ethernet, Frame Relay, not to mention the X.25 packet switching are considered even such a simple analysis as outdated technology that does not meet current realities.

Based on the study, proposed a comprehensive indicator of functional efficiency ABS. Structure of construction index is that it combined two major characteristics of the system:

- BIn for IB in terms of hybrid security threats to the components, IB, CB, BI BIn in ABS;
- likelihood required for achieving goal with the necessary measure of confidentiality in certain environmental conditions and at a certain level of influence of internal random factors;
- the cost of achieving the goal of a necessary and likely economic cost of the building and investing in the ABS TZZI CISS considering the required service quality indicator data.

Thus, the rate of functional efficiency of the network ABS-based model multivariate analysis given by the expression:

$$W(u_i) = \frac{n^{(u_i)} - t^{(u_i)}}{n^{(u_i)}} \times B^{(u_i)} \times P_{right\ receipt}^{(u_i)} \times W_{effinv} \times W_{norm}, \quad (4.33)$$

where: $W(u_i)$ — ABS network performance indicator, the strategy chosen method (increase reliability) u_i ;

$n^{(u_i)}$ — the number of bits of information in the package chosen strategy u_i ;

$t^{(u_i)}$ — the delivery package during u_i chosen strategy;

$B^{(u_i)}$ — the stability of security in the chosen strategy u_i , based on the results of evaluation of the stability offered by express method and results evaluation hybrid countering threats to security components: IB, CB, IB BIn in ABS (4.29);

$P_{right\ receipt}^{(u_i)}$ — the probability of correct packet delivery with the chosen strategy;

U — the set of admissible strategies (methods for increasing reliability, used in network ABS-based IP Internet);

W_{effinv} — multi-rate efficiency, calculated by the proposed investment in TZZI (see subsection. 4.1);

W_{norm} — normalized multi-performance.

This approach allows without significant economic, computing and human resources to consider not only technical, but also economic parameters TZZI ABS, to more precisely evaluate its functional effectiveness, consider the results of studies scaling network ABS choice TZZI to build and maintain the CISS, analysis countering threats on component safety: IB, CB, BI BIn in ABS, hybridization and their synergies, minimize cost and effective control over the software CISS ABS.

The technique of evaluating functional efficiency through integrated ABS indicator evaluating the quality of service facilities for the safety of ABS Bin lets emergent properties based on the synthesis of complex index of efficiency of investment in ABS TZZI, results evaluation threats to information resources and infrastructure ABS, their hybridization and synergism, assessment results and rapid method stability and efficiency of the program (software and hardware) implementation cryptographic algorithms.

4.3 The findings of the fourth section

Thus, in the fourth section, the results of research related to the development of evaluation method investment in IB BIn in ABS, which differs from the known complexation economic indicators of investment in IB BIn in ABS considering synergy and hybridity attacks on security components, IB, CB, BI.

To evaluate the quality of service facilities for the safety of ABS BIn proposed method of estimating the functional efficiency of data exchange network ABS, which is based on a simple multivariate analysis, which takes into account both technical data networks (data rate and the probability of the delivery package and so on), safety technical information security, and economic parameters (price scale, service network, the efficiency of investment in safety, etc.).

1. A method for evaluating the effectiveness of investments in the banking information security in automated banking systems which is based on a composite index investing to optimize the cost of funds for the construction of a system of information security in terms of hybrid threats of information security cyber-security and safety information. The practical implementation of the method allow to assess key indicators of investment in IT security given BIn synergistic evaluation of threats IB, CB, BI.

2. A method for evaluating the functional efficiency of data exchange network ABS, which is based on a simple multivariate analysis, which takes into account both technical data networks (data rate and the probability of the delivery package and so on.), Safety technical protection of information, as and economic parameters (price scale, service network, the efficiency of investment in safety, etc.). The proposed method of estimating the functional efficiency of ABS allows without significant time and cost to conduct expert evaluation of ABS for users to use the results of the evaluation of the functional efficiency of ABS for its scale, improve technical performance network ABS information security of banking information.

References in Chapter 4

1. *G.P. Leonenko, A.Yu. Yudin* Problemy obespecheniya informatsionnoy bezopasnosti sistem kriticheski vazhnoy informatsionnoy infrastruktury Ukrainy//Information Technology and Security, № 1 (3), p. 44–48, 2013.
2. *A.A. Sinyak, N.E. Gubenko* Analiz metodov otsenki effektivnosti zatraat v informatsionnuyu bezopasnost'. IUS i KM. Section 4. Web-tekhnologii i IB, p. 444–446, 2012.
3. *V.P. Pervadchuk, V.A. Beletskiy* Otsenka effektivnosti investirovaniya v informatsionnuyu bezopasnost' predpriyatiya na osnove nechetkikh mnozhestv//Vestnik IzhGTU, № 1 (49), p. 51–53, 2011.
4. *E. V. Zubareva, A.A. Babenko* Metody otsenki investitsiy v informatsionnuyu bezopasnost' predpriyatiya. URL: www.volsu.ru/download.php?id=000028639-1.pdf. Accessed on: 4.12.2017.
5. *K. G. Khomyakov, L. V. Kanitskaya* Otsenka effektivnosti investitsiy v kompleksnye sistemy zashchity informatsii kompaniy neftegazovogo kompleksa

- dlya prinyatiya vzveshennogo investitsionnogo resheniya//*Ekonomika. Fundamental'nye issledovaniya*, Ed. № 2, p. 5173–5177, 2015.
6. *I. M. Azhmukhamedov, T. B. Khanzhina* Otsenka ekonomicheskoy effektivnosti mer po obespecheniyu informatsionnoy bezopasnosti//*Vestnik AGTU. Ser.: Ekonomika*, Ed. № 1, p. 185–190, 2011.
 7. *S. A. Petrenko* Otsenka zatrat na kiberbezopasnost'//*Trudy ISA RAN*, v. 27, p. 235–265, 2006.
 8. *N. Kozhokaru* Effektivnost' investitsiy v oblasti informatsionnoy bezopasnosti. URL: <http://www.securitylab.ru/bitrix/exturl.php?goto=http://1.bp.blogspot.com/-7Lhsq9eFw7U/VhZrMFnOLJI/AAAAAAAAAHqk/AH-T9E2u8R9E/s1600/risk-taxonomy.bmp>. Accessed on: 4.12.2017.
 9. *E. N. Efimov, G. M. Lapitskaya* Otsenka effektivnosti meropriyatiy informatsionnoy bezopasnosti v usloviyakh neopredelennosti//*Biznes-Informatika. Matematicheskie metody i algoritmy resheniya zadach biznes-informatiki*, Ed. № 1 (31), p. 51–57, 2015.
 10. *S. Evseev* Sinergeticheskaya model' otsenki bezopasnosti bankovskoy informatsii//*Informatsionnaya bezopasnost'*, № 4 (24), p. 104–118, 2016.
 11. *S. Evseev* Model' narushitelya prav dostupa v avtomatizirovannoy bankovskoy sisteme na osnove sinergeticheskogo podkhoda//*Informatsionnaya bezopasnost'*, № 2 (26), p. 110–120, 2017.
 12. *S. S. Zharinova, A. A. Babenko* Optimizatsiya investitsiy v informatsionnuyu bezopasnost' predpriyatiya//*GU-UNPK: Informatsionnye sistemy i tekhnologii*, Vyp. 3 (83), p. 114–123, 2014.
 13. *S. S. Zharinova, A. A. Babenko* Model' effektivnosti investitsiy v informatsionnuyu bezopasnost' predpriyatiya. URL: www.volsu.ru/download.php?id=000026221-1.pdf. Accessed on: 4.12.2017.
 14. *FGBOU VPO "MG TU im. N. E. Bauman"*, El № FS 77–48211, Ed. № 3, p. 267–287, 2016.
 15. *S. Evseev* Otsenka effektivnosti investitsiy v bezopasnost' organizatsiy bankovskogo sektora na osnove sinergeticheskoy modeli ugroz//*Sistemy obrabotki informatsii*, № 2 (148), p. 88–94, 2017.
 16. *O. G. Korchenko, O. E. Arkhipov, Yu. O. Dreys* Otsenka ushcherba natsional'noy bezopasnosti Ukrainy v razvitii utechki gosudarstvennoy tayny. – K.: SBU, 2014.
 17. *R. V. Grishchuk, Yu. G. Danik* Osnovi kiberbezpeki/za zag. red. prof. Yu. G. Danika. – Zhitomir: ZHNAEU, 2016.
 18. *A. O. Korchenko, L. M. Skachek, V. O. Khoroshko* Bankovskaya bezopasnost'. – Kiev: PVP "Zadruga", 2014.
 19. *S. Evseev, O. Korol'* Kompleksnyy pokazatel' effektivnosti investitsiy v bezopasnost' bankovskoy informatsii na osnove sinergeticheskoy modeli

- ugroz. VI Mezhdunarodnaya nauchnaya konferentsiya "Informatsiya, kommunikatsiya, obshchestvo 2017". – Slavskoe, p. 18–19, 2017.
20. A. Arkhipov Primenenie ekonomiko-stoimostnykh modeley informatsionnykh riskov dlya otsenivaniya predel'nykh ob'emov investitsiy v bezopasnost' informatsii//Zashchita informatsii, vol. 17, № 3, p. 211–218, 2015.
21. S. Goloshchapov 100 GB Ethernet: osnovnye printsipy. URL: www.last-mile.su/journal/article/2820. Accessed on: 4.12.2017.
22. S. P. Evseev, D. V. Sumtsov, O. G. Korol', B. P. Tomashevskiy Analiz effektivnosti peredachi dannykh v komp'yuternykh sistemakh s ispol'zovaniem integrirovannykh mekhanizmov obespecheniya nadezhnosti i bezopasnosti//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, № 2/2 (44), p. 45–49, 2010.
23. S. P. Evseev, S. E. Ostapov, R. V. Korolev Ispol'zovanie mini-versiy dlya otsenki ustoychivosti blochno-simmetrichnykh shifrov//Bezopasnost' informatsii, Vol. 23, № 2, p. 100–108, 2017.
24. I. D. Gorbenko, V. I. Dolgov, I. V. Lisitskaya, R. V. Oleynikov Novaya ideologiya otsenki stoykosti blochnykh simmetrichnykh shifrov k atakam differentsial'nogo i lineynogo kriptanaliza//Prikladnaya radioelektronika, vol. 9, № 3, p. 312–320, 2010.
25. V. I. Dolgov, I. V. Lisitskaya Metodologiya otsenki stoykosti blochnykh simmetrichnykh shifrov k atakam differentsial'nogo i lineynogo kriptanaliza. Monografiya. – Khar'kov: Publishing house «Fort», 2013.
26. I. V. Lisitskaya A new method for assessing the stability of block symmetric ciphers for attacks of differential and linear cryptanalysis//Sistemy obrabotki informatsii, ed. 4 (94), p. 167–173, 2011.
27. I. V. Lisitskaya Metodologiya otsenki stoykosti blochnykh simmetrichnykh shifrov. URL: <https://cyberleninka-.ru/article/n/metodologiya-otsenki-stoykosti-blochnykh-simmetrichnykh-shifrov>. Accessed on: 4.12.2017.
28. I. V. Lisitskaya Bol'shie shifry – sluchaynye podstanovki. Sravnenie differentsial'nykh i lineynykh svoystv shifrov, predstavlenykh na ukrainskiy konkurs, i ikh umen'shennykh modeley. URL: <https://cy-berleninka.ru/article/n/bolshie-shifry-sluchaynyepod-stanovki-sravnenie-differentsialnyh-i-lineynykh-svoystv-shifrov-predstavlenykh-na-ukrainskiy-konkurs-i-ih>. Accessed on: 4.12.2017.
29. I. V. Lisitskaya, K. E. Lisitskiy, M. Yu. Rodinko, I. A. Golovko, I. I. Zharikov, M. A. Kornienko, M. V. Kuleba Eksperimental'nye dannye po opredeleniyu dinamicheskikh pokazateley prikhoda blochnykh simmetrichnykh shifrov k sostoyaniyu sluchaynosti//Radioelektronika, informatika, upravlenie, № 1, p. 129–141, 2017.

30. I. V. Lisitskaya, A. A. Nastenko Bol'shie shifry — sluchaynye podstanovki//Mezhvedomstvennyy nauchn. tekhnicheskiiy sbornik «Radiotekhnika», Ed. 166, p. 50–55, 2011.
31. L. Soroka, A. Kuznetsov, I. Moskovchenko, S. Isaev Issledovanie differentsial'nykh svoystv blochno-simmetrichnykh shifrov//Sistemy obrabotki informatsii, edition 6 (87), p. 286–295, 2010.
32. I. Lisitskaya, A. Kuznetsov, S. Isaev Lineynye svoystva blochnykh simmetrichnykh shifrov, predstavlenykh na ukrainskiy konkurs//Prikladnaya radioelektronika: nauchno-tekhn. zhurnal, vol. 10, № 2, p. 135–140, 2011.
33. I. V. Lisitskaya, T. A. Grinenko, S. Yu. Bessonov Analiz differentsial'nykh i lineynykh svoystv shifrov rijndael, serpent, threefish pri 16-bitnykh vkhodakh i vykhodakh//Vostochno-Evropeyskiy zhurnal peredovykh tekhnologiy, p. 50–54, 2015.
34. G. Piret, F.-X. Standaert Provable security of block ciphers against linear cryptanalysis: a mission impossible?//Designs, Codes and Cryptography, V. 50, № 3, p. 325–338, 2009.
35. B. Collard, F.-X. Standaert Experimenting linear cryptanalysis”, Advanced Linear Cryptanalysis, V. 116, p. 90–117, 2011.
36. L. R. Knudsen Practically Secure Feistel Ciphers. Proc. Fast Software Encryption. – Cambridge, 1993, Springer, V. 809, p. 211–221, 1994.
37. A. Rukhin, J. Soto A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800–22, 09.2000, 164 p.
38. K. Shannon Raboty po teorii informatsii i kibernetike. – M.: IL, 1963.
39. S. P. Evseev Metodologiya otsenivaniya bezopasnosti informatsionnykh tekhnologiy avtomatizirovannykh bankovskikh sistem Ukrainy//Ukrainian Scientific Journal of Information Security, vol. 22, issue 3, p. 297–309, 2016.
40. S. Evseev, O. Korol', A. Sochneva Analiz otsenki riskov kiberbezopasnosti bankovskoy informatsii. Sbornik nauchnykh trudov NAU “Zashchita informatsii”, ed. 23, p. 109–128, 2016.
41. S. Evseev, A. Sochneva, O. Korol', V. Abdulaev Analiz metodik otsenki riskov narusheniya bezopasnosti bankovskoy informatsii//Izvestiya Vysshikh tekhnicheskikh uchebnykh zavedeniy Azerbaydzhana. Vol. 19, № 2 (106), p. 77–86, 2017.
42. A. P. Smirnov Funktsional'naya effektivnost'. URL: <https://www.ngpedia.ru/id625108p1.html>. Accessed on: 4.12.2017.
43. MSE-T E.800 Opredelenie terminov, otnosyashchikhsya k kachestvu obsluzhivaniya. URL: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.800-200809. Accessed on: 4.12.2017.

44. ISO 9000:2015 (ru) Quality management systems — Fundamentals and vocabulary. URL: <https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en>. Accessed on: 4.12.2017.
45. Standart GOST RV 51987 “Informatsionnaya tekhnologiya, kompleks standartov na AS”. URL: <http://gearletitbit.weebly.com/blog/gost-rv-51987-2002>. Accessed on: 4.12.2017.
46. G. G. Yanovskiy Kachestvo obsluzhivaniya v setyakh IP. URL: niits.ru/public/2008/2008-006.pdf. Accessed on: 4.12.2017.
47. Shrinivasa Vegeshny Kachestvo obsluzhivaniya v setyakh IP. URL: http://it-ebooks.ru/publ/cisco/cisco_ip_quality_of_service/11-1-0-293. Accessed on: 4.12.2017.
48. Quality of Service (QoS) in a network with software (SDN): an overview. URL: <https://doi.org/10.1016/j.jnca.2016.12.019>. Accessed on: 4.12.2017.
49. A single quality of service (QoS) survey in OPS/OBS networks. URL: <https://doi.org/10.1016/j.yofte.2017.05.016>.
50. Modeling of network access protocols for network quality analysis. URL: 10.1109/ISORC.2015.47. Accessed on: 4.12.2017.
51. S. P. Evseev, S. E. Ostapov, Kh. N. Rzaev, V. I. Nikolaenko Otsenka obmena dannymi v global'nykh vychislitel'nykh setyakh na osnove kompleksnogo pokazatelya kachestva obsluzhivaniya seti//Nauchnyy zhurnal Radioelektronika, informatika, upravlenie, № 1 (40), p. 115–128, 2017.
52. Quality of Service: Implementation of a new structure and new measurement methodology. URL: Resource Access Mode: 10.1109/INFOMAN.2017.7950439.
53. A. I. Kayashev Analiz pokazateley nadezhnosti lokal'nykh komp'yuternykh setey/A. I. Kayashev, P. A. Rakhman, M. I. Sharipov//Vestnik UGATU, Ufa, Vol. 17, № 5 (58), p. 140–149, 2013.
54. S. P. Evseev Analiz effektivnosti peredachi dannykh v komp'yuternykh sistemakh s ispol'zovaniem integrirovannykh mekhanizmov obespecheniya nadezhnosti i bezopasnosti/S. P. Evseev, D. V. Sumtsov, O. G. Korol', B. P. Tomashevskiy//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, № 2/2 (44), p. 45–49, 2010.
55. S. P. Evseev Integrirovanny pokazatel' kachestva obsluzhivaniya pol'zovateley global'nykh vychislitel'nykh setey. VIII Mezhdunarodnaya nauchno-tekhnicheskaya konferentsiya “Informatsionno-komp'yuternye tekhnologii – 2016”. – Zhitomir, p. 17–18, 2016.
56. S. V. Lenkov, D. A. Peregudov, V. A. Khoroshko Metody i sredstva zashchity informatsii: Nesanktsionirovannoe poluchenie informatsii/edited by V. A. Khoroshko. – K.: Ariy, v. 1, 2008.

57. S. V. Lenkov, D. A. Peregodov, V. A. Khoroshko Metody i sredstva zashchity informatsii: Informatsionnaya bezopasnost'/edited by V. A. Khoroshko. – K.: Ariy, v. 2, 2008.
58. Yu. I. Gorbenko, I. D. Gorbenko Infrastruktura otkrytykh klyuchey. Elektronnyaya tsifrovaya podpis'. Teoriya i praktika. – Khar'kov: Fort, 2010.
59. I. D. Gorbenko, Yu. I. Gorbenko Prikladnaya Kriptologiya. – Khar'kov: Fort, 2012.
60. A. A. Kuznetsov, R. V. Oleynikov, Yu. I. Gorbenko, A. I. Pushkarev, O. V. Dyrida, I. D. Gorbenko Obosnovanie trebovaniy, postroeniya i analiz perspektivnykh simmetrichnykh kriptopreobrazovaniya na osnove blochnykh shifrov//Vestnik Natsional'nogo universiteta "Lvovskaya politehnika". Komp'yuternye sistemy i seti, № 806, p. 124–141, 2014.
61. B. Shnayer Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke S. – M.: Publisher TRIUMF, 2002.
62. N. A. Moldovyan, A. A. Moldovyan, M. A. Eremeev Kriptografiya: ot primitivov k sintezu algoritmov. – SPb.: BKhV, Peterburg, 2004.
63. S. E. Ostapov, S. P. Evseev, O. G. Korol' Tekhnologii zashchity informatsii. – Chernovtsy: Publisher "RODOVID", 2014.
64. V. Stollings Kriptografiya i zashchita setey: printsipy i praktika; ed. 2. – M.: ID "Vil'yams", 2001.
65. B. Sklyar Tsifrovaya svyaz'. Teoreticheskie osnovy i prakticheskoe primeneniye. ed. 2. – M.: Publisher "Vil'yams", 2003.
66. S. P. Evseev, D. V. Sumtsov, O. G. Korol', B. P. Tomashevskiy Analiz effektivnosti peredachi dannykh v komp'yuternykh sistemakh s ispol'zovaniem integrirovannykh mekhanizmov obespecheniya nadezhnosti i bezopasnosti// Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, № 2/2(44), p. 45–49, 2010.
67. O. G. Korol' Otsenka kachestva obsluzhivaniya global'noy seti na osnove tekhnologiy Ethernet s pomoshch'yu kompleksnogo pokazatelya//Sistemy obrabotki informatsii, № 2(148), p. 88–94, 2017.

CHAPTER 5. Verification and investigation of developed models and methods. Construction methodology of information security system of banking information in the automated banking system

5.1 Comparative analysis of the transfer banking information efficiency in automated banking systems developed through comprehensive measure of evaluating the quality of service objects automated banking system to ensure the safety of bank information

To increase the values of the functional efficiency of the computer network in [1] Considered various ways to manage data exchange, without feedback from r -detecting multiple errors; without feedback correcting t -multiple error. And most used management protocols, with critical feedback and continuous transfer rate (VZZ_{BPK}) “Back-to- N ”; with a decisive and positive feedback receipt (VZZ_{PK}).

The investigations in [1, 2, 3] Showed that to maximize the functional efficiency of IP-based networks need to use protocols of critical feedback and continuous transfer rate (VZZ_{BPK}) “Back-to- N ”; with a decisive and positive feedback receipt (VZZ_{PK}).

In addition, a detailed study of the statistical properties of sequences errors in real channels [4, 5, 6, 7, 8, 9] Showed that the errors are dependent and have a tendency to Cohesion (packaging), that between them there is a dependence — correlation. Most of the time the information is no distortion channels of communication, and in some moments there condensation errors, so-called packets (packs, groups) errors. Inside the packet error probability of error is much higher than average probability of error calculated for a considerable time transmission.

In such circumstances, how to protect, the best hypothesis for independent errors are ineffective when used in real communication channels. To account for the statistical properties of sequences of real errors in communication channels consider the model of discrete channel with memory.

The model in the output bit error probability instead P_0 must specify the following four channel parameters:

- the probability of packet errors — P_{error} ;
- the probability of errors inside the package — P_ε ;
- expectation m_{in} length packet errors;

– standard deviation σ_{ln} length packet errors.

In the calculations taken: $P_{error} = 10^{-5} \div 10^{-2}$; $P_{\varepsilon} = 0.8$; $m_{ln} = 10$; $\sigma_{ln} = 2$.

For network ABS with critical feedback and continuous transmission frame “Return-to- N ” value performance indicator is given by:

$$W(u_3) = \frac{n^{(u_3)} - t^{(u_3)}}{n^{(u_3)}} \times B^{(u_3)} \times P_{right receipt}^{(u_3)} \times W_{effinv} \times W_{norm}, \quad (5.1)$$

where: $W(u_i)$ — Network performance indicator ABS, the strategy chosen method (increase reliability) u_i ;

$n^{(u_i)}$ — the number of bits of information in the package chosen strategy u_i ;

$t^{(u_i)}$ — the delivery package during t u_i chosen strategy;

$B^{(u_i)}$ — the stability of security in the chosen strategy u_i ;

$P_{right receipt}^{(u_i)}$ — the probability of correct packet delivery with the chosen strategy;

U — the set of admissible strategies (methods for increasing reliability, used in network ABS-based IP Internet);

W_{effinv} — multi-rate performance;

W_{norm} — normalized multi performance.

$$\begin{aligned} m_t^{(u_3)} &= \frac{n}{C} + \frac{L}{V_p} + t_{encrypt} + t_{decrypt} + \\ &+ \frac{\sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_p)^{n+i} \right] \cdot \left[\Phi \left(\frac{i+1-m_{ln}}{\sigma_{ln}} \right) - \Phi \left(\frac{i-m_{ln}}{\sigma_{ln}} \right) \right] \right\}}{1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_p)^{n+i} \right] \cdot \left[\Phi \left(\frac{i+1-m_{ln}}{\sigma_{ln}} \right) - \Phi \left(\frac{i-m_{ln}}{\sigma_{ln}} \right) \right] \right\}} \times \\ &\times \left\{ 1 - \frac{1}{2^r} \cdot \left[\frac{1}{2} - \Phi \left(\frac{r+1-m_{ln}}{\sigma_{ln}} \right) \right] \right\} \times \left(\frac{n+s}{C} + 2 \frac{L}{V_p} \right), \\ K &= \left[\Phi \left(\frac{i+1-m_{ln}}{\sigma_{ln}} \right) - \Phi \left(\frac{i-m_{ln}}{\sigma_{ln}} \right) \right]; \end{aligned} \quad (5.2)$$

$$P_{prp}^{(u_3)} = \frac{1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_p)^{n+i} \right] \times K \right\}}{1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_p)^{n+i} \right] \times K \right\} \times \left\{ 1 - \frac{1}{2^r} \times \left[\frac{1}{2} - \Phi \left(\frac{r+1-m_{ln}}{\sigma_{ln}} \right) \right] \right\}}. \quad (5.3)$$

For network ABS with a decisive and positive feedback values of frame receipt efficiency is defined as:

$$W(u_4) = \frac{n^{(u_4)} - t^{(u_4)}}{n} \times B^{(u_4)} \times P_{right receipt}^{(u_4)} \times W_{effinv} \times W_{norm}, \quad (5.4)$$

where:

$$t^{(u_4)} = \frac{n+s}{C} + 2 \frac{L}{V_p} + t_{encrypt} + t_{decrypt} + \frac{n}{C} \times$$

$$\times \frac{\sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_p)^{n+i} \right] \cdot \left[\Phi \left(\frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi \left(\frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}}{1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_p)^{n+i} \right] \cdot \left[\Phi \left(\frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi \left(\frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}} \times \quad (5.5)$$

$$\times \left\{ 1 - \frac{1}{2^r} \cdot \left[\frac{1}{2} - \Phi \left(\frac{r+1-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\},$$

$$K = \left[\Phi \left(\frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi \left(\frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right];$$

$$P_{right receipt}^{(u_4)} = 1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_p)^{n+i} \right] \cdot K \right\} \times \quad (5.6)$$

$$\times \frac{1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_p)^{n+i} \right] \cdot K \right\} \cdot \left\{ 1 - \frac{1}{2^r} \cdot \left[\frac{1}{2} - \Phi \left(\frac{r+1-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}^N}{1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_p)^{n+i} \right] \cdot K \right\} \cdot \left\{ 1 - \frac{1}{2^r} \cdot \left[\frac{1}{2} - \Phi \left(\frac{r+1-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}},$$

Fig. 5.1, 5.2 These results assess the functional efficiency of the computer network ABS multifactorial indicator of normalized on the basis of BSC.

When conducting cryptographic strength research used evaluation methods based on entropy method and the results of the methodology for assessing the economic costs based on the methodology FAIR (research results are presented in [2] Fig. 5.1).

Initial data for the study are: technology 1 *Gbit Ethernet*, 10 *Gbit Ethernet*, with critical feedback and continuous transmission frame

“Return-to- N ”, $W_{synerg}^{IB,KB,BI} = 0.0022839$, $t_{encrypt} = t_{decrypt} = 0.01$ s, $P_C^{AES} = 0.95454$,

$P_C^{Kalyna256} = 0.9454519$, $P_C^{3DES} = 0.812043$, $n = 1518$, $C = 36000$, $P_{right receipt} = 0.99$.

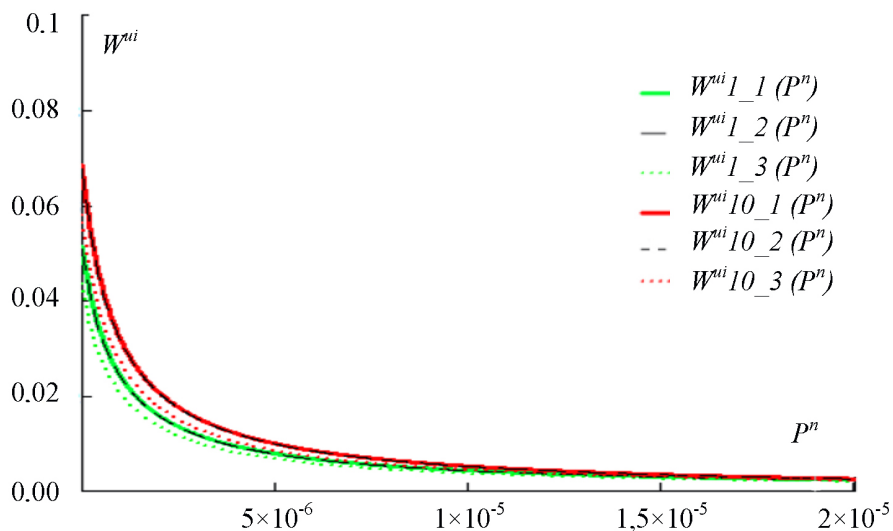


Fig. 5.1. The research results of the functional efficiency of the network ABS critical feedback and continuous transmission frame "Return-to-N" using the technique FAIR

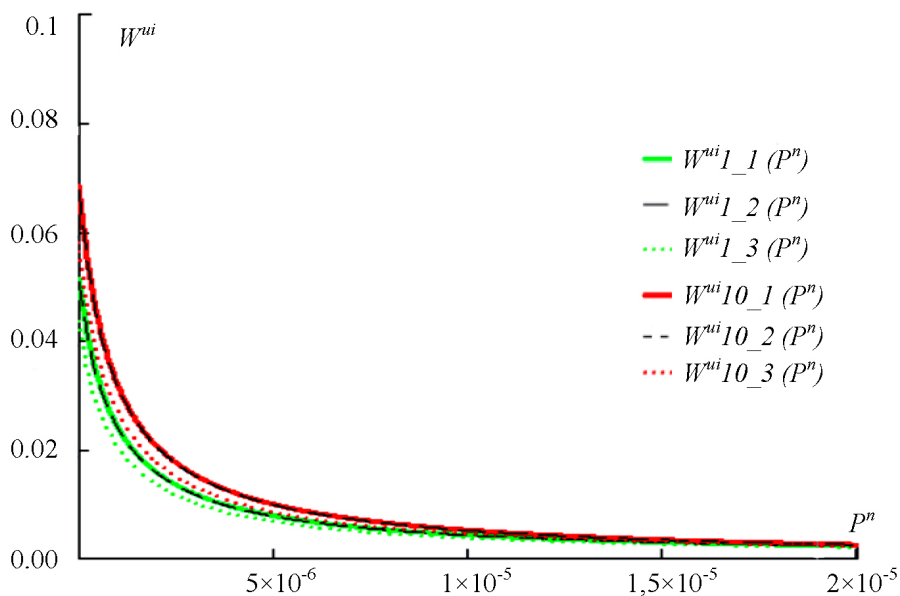


Fig. 5.2. The research results of the functional efficiency of the network ABS critical feedback and continuous transmission frame "Return-to-N" using methods of evaluating investment

When conducting research (Fig. 5.2) cryptographic strength BSC evaluation performed on the basis of the proposed rapid method of assessing the economic costs TZZI made on the proposed methodology (see subsection 4.1.1). Initial data for the study are: technology 1 Gbit Ethernet, 10 Gbit Ethernet, with critical feedback and continuous transmission frame “Return-to-N”, $W_{synerg}^{IB,KB,BI} = 0.0022839$, $t_{encrypt} = t_{decrypt} = 0.01$ s, $P_C^{AES} = 0.95454$, $P_C^{Kalyna256} = 0.9454519$, $P_C^{3DES} = 0.812043$, $n = 1518$, $C = 36000$, $P_{right\ receipt} = 0.99$.

Comparative analysis of Fig. 5.1, 5.2 showed its adequacy and flexibility. The technique allows to unify the assessment of the effectiveness of data exchange on a global protocol IP-based networks, taking into account economic costs of hardware and software tools and technologies that provide the required performance security and reliability of functional efficiency ABS OPS and necessary values of service quality IP-based networks, which OPS is the basis NSMEP. Practical use of injected indicator will more accurately assess the effectiveness of communication protocols used in global IP-based networks protocols ABS. In addition, this approach will solve the problem in more detail with scaling and expandability network ABS because it includes not only technical, but also economic indicators functional efficiency, it is very important to ensure the required quality of service users ABS. Expressions efficacy data network ABS at different ways of managing data exchange yield comparative quantitative assessment of the stability program (software and hardware) implementation TZZI, the possible implementation of hybrid threats BI in ABS, efficiency investments in TZZI, integrated performance indicator using various protocols control data exchange networks based on Ethernet-technology.

5.2 Generalization of the results: the methodology of synthesis and analysis of the proposed models and methods of information security of banking information

In modern terms, as shown, an important role in ensuring national security of Ukraine and especially its economic component belongs processes to ensure information security in the banking sector. And system-key role in building a system of information security of banking information as part of national information resources of the state, plays a theory and practice in which scientific and methodological base is the foundation for sound and effective management decisions entities providing information security at all levels.

The revolutionary changes of the last decades that have taken place in the banking sector led to the unification of information and computer networks into a

single information and cyberspace. Integration processes led to the development of automated banking systems (ABS), which significantly expanded the range of electronic services to government and commercial banks in the world and Ukraine. As a result, substantially transformed and threats in such a state of national information resources as banking information (BIn).

Threats have become signs of hybridity. From a purely informational threats, cyber security and information security BIn displays signs of hybridity began to occur as a result of simultaneous action on the object of protection — BIn in ABS, due to the emergence of synergy effects.

It is known that the methodological basis of any security is a key component of the theory of safety and based on the methods and models necessary and sufficient for investigation of security problems and solve practical problems relevant destination. So now in the field of information security, there is quite a large number of methodologies. In particular, the analysis methodologies related to development of scientific basis for the synthesis of these security systems [10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20]:

- Synthesis and analysis of differential-game models and methods of modeling processes for government cyber information resources [10];
- Assess the level of protection of public resources from social and technical attacks [11];
- Assessment of damage to national security in the sphere of state secrets [12];
- Construction and safe use of wireless sensor networks with random parameters network [13];
- Protection of state information resources [14];
- Analysis of complex technical information security [15];
- Risk analysis tree ID state information resources [16];
- Building systems detect anomalies generated by cyber attacks [17];
- Systems analysis and risk the loss of information resources [18];
- Comprehensive protection of people and social groups from the negative information and psychological impact [19];
- Adaptive systems security risk assessment resources information systems [20] etc.

However, the methodology analyzed do not include synergies and signs of hybridity security threats to the components in the BIn ABS, namely [21, 22, 23]. Information security (IS), Cybersecurity (KBrB), security information (BI). So they all need radical revision in the part concerning the creation of a methodological basis for constructing a system of information security BIn in ABS as Ukraine in general and in particular the world.

Based on the analysis [24, 25, 26, 27, 28] Can be argued that one of the priorities of raising IB BIn in ABS particular and further stabilization IB state as a whole is fundamentally new solution to the problem of IB Organizations banking sector State (OPS) through the creation of modern methods and means of protecting BIn of hybrid attack from complexation characteristics of threats to information security, KBrB, BI BIn in the ABS, the technical facilities of its infrastructure. Thus, significant research results in solving the problems of the state IB and disclosure of its individual components in OPS obtained in scientific studies [25, 26, 28, 29, 30, 31, 32] et al., But despite this problem is actual not only for Ukraine but also for the international community.

Based on the common system approach [28, 30, 31, 32] And the need to implement an integrated approach to developing advanced systems for IB BIn in ABS in terms of hybridization and integration of information security threats, KBrB, BI now there is an objective contradiction between high standards of practice to ensure information security BIn in ABS and imperfect, and sometimes the lack of effective scientifically grounded methodological bases of support.

The analysis of the regulations on organization building a system for IB BIn in ABS in [21, 22, 23, 33, 34, 35, 36, 37] Showed that until now considered only certain components of the methodology of evaluation of information security technologies used in OPS. They are based on models of security — confidentiality, integrity and availability (model KTSD). Applying the model does not account KTSD integral part of banking transactions — service authentication — BIn condition in which the information provides authentication source (authorized user and/or process) of information. In addition, no synergistic approach to risk analysis, assessment methodology common information technology security standards in the banking sector does not allow timely develop appropriate policies, new approaches and measures to ensure information security BIn. known that early detection and risk analysis is an integral part of the problem for IB BIn. In fact, the risk is an integral assessment of how well existing data protection (ZZI) can withstand attacks on BIn in ABS. In practice there are two main groups of methods for assessing security risks [38, 39, 40]. The first group allows you to set the level of risk by evaluating the extent to defined set of requirements for information security. The second is based on determining the probability of attacks and levels of damage. But both groups of methods also do not include attacks on hybridity modern OPS, so do not allow them to respond to manifestations.

A promising approach for IB BIn in ABS is the simultaneous combination of rational and organizational measures and technical means to ensure information security, and BI KBrB that ultimately displayed on the investment bank, invested in security. This integration of the security forces and means in each case is not effective and one that does not guarantee achievement of expected synergies security [41, 63].

Thus, as is clear from the above, based on existing methodological apparatus is problematic, and in some cases impossible to achieve the goal of the study.

Based on the known approach to building methodologies [10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20] Based research [41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 62, 63] Proposed a radically new methodology for constructing systems for IS BIn in ABS.

It contains five stages (Fig. 5.3, 5.4):

- 1) determine the probability of the impact of threats IB, KBrB, BI information security Bin;
- 2) a generalized index of IS BIn in ABS;
- 3) evaluating the effectiveness of investment in information security in the BIn ABS;
- 4) construction of the integrated mechanisms to ensure the confidentiality, integrity, authenticity and credibility BIn in ABS;
- 5) determine the status and forming strategies IS BIn in ABS.

Stage 1. *Determining the impact probability of threats IB, KBrB, BI information security BIn.* In the first stage, based on the argument that the threat IS, CS, SI have the opportunity to influence the various security services (confidentiality, integrity, availability, authenticity) with varying intensity experts IB solve the problem concerning the valuation of weighting coefficients and form classification of threats from proposed classifier [33]. Classifier components are:

- part of a security BIn OPS ABS: IB (01), BI (02) KBrB (03);
- the nature areas: regulatory (01), organizational (02), engineering (03);
- the main features of information: privacy (01), integrity (02), availability (03), authenticity (04);
- the hierarchy of infrastructure ABS: FL — physical layer (01), NL — network layer (02), OSL — operating systems level (OS) (03), DBL — database management systems level (04), BL — banking technology applications and services level (05). The set of information security threats, CS, SI BIn at the ABS prompted use of resources [61].

To determine the probability of occurrence of PI i -th threats using data from the table 5.1.

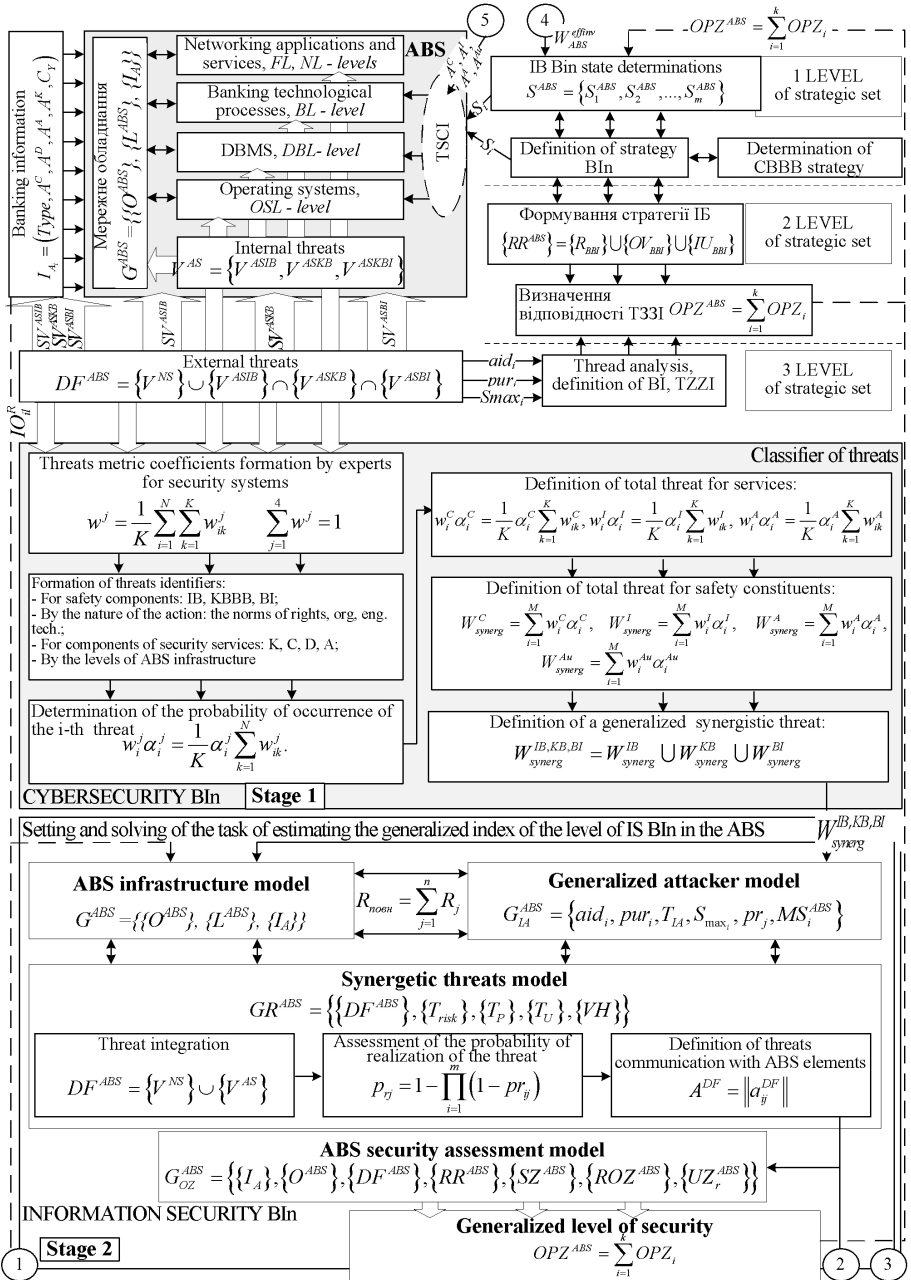


Fig. 5.3. Scheme methodology of constructing a system of information security in automated banking systems

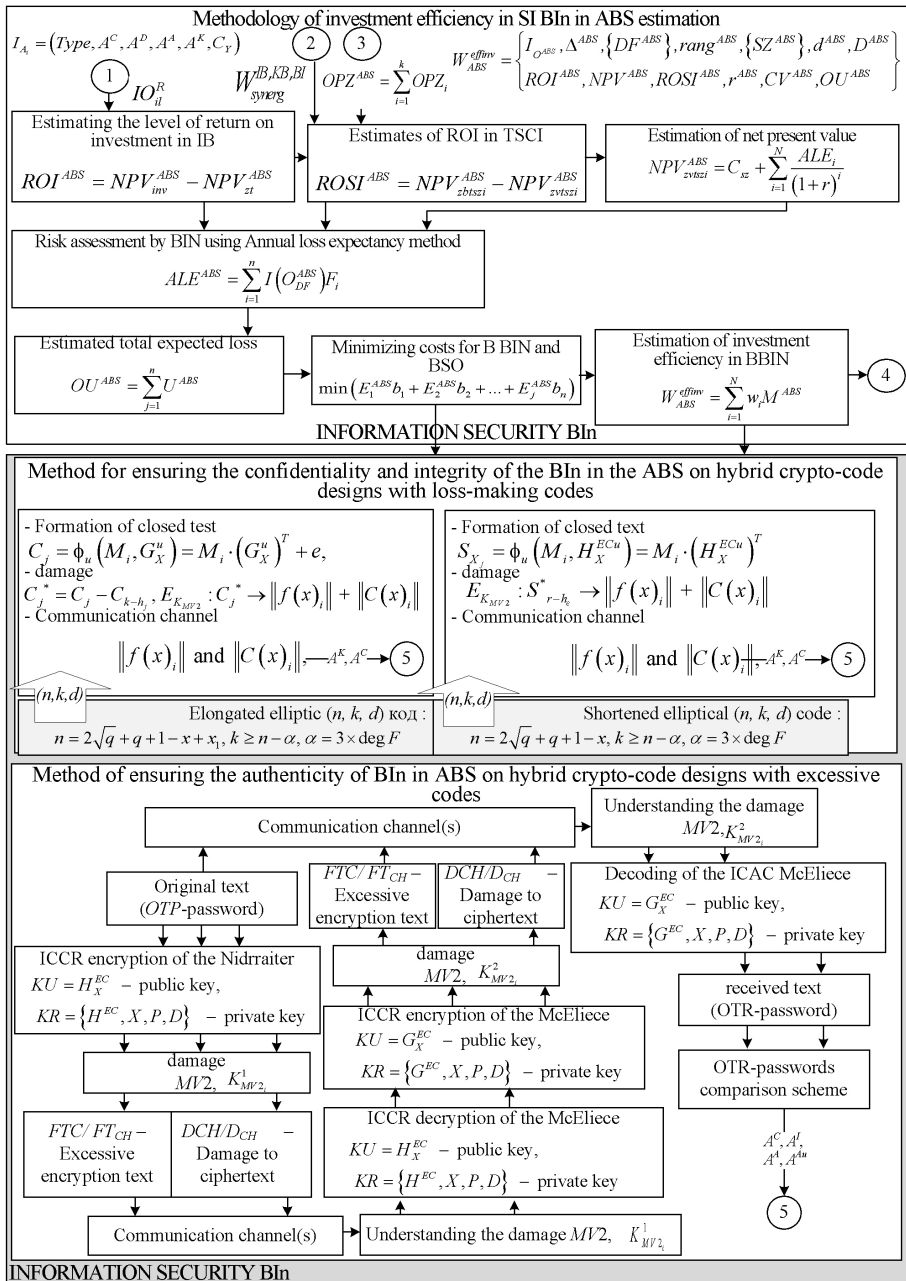


Fig. 5.4. Scheme methodology of constructing a system of information security in automated banking systems

Table 5.1. — Table determine the potential threats, depending on the frequency of their manifestation

P_i	The incidence of threats
0.67	threat appears no more than once every 5 years
0.133	threat appears no more than once a year
0.2	threat appears no more than once a month
0.267	threat appears no more than once a week
0.333	threat manifests itself daily

Definition of implementation of each i -th threat considering the frequency of its occurrence is under expression:

$$w_i = w_i^C P_i \cup w_i^I P_i \cup w_i^A P_i \cup w_i^{Au} P_i, P_i = 1. \quad (5.7)$$

Determining the likelihood of some threats on certain security services carried out as:

$$W^C = \sum_{i=1}^N w_i^C P_i \quad \text{— for confidentiality;}$$

$$W^I = \sum_{i=1}^N w_i^I P_i \quad \text{— for integrity;}$$

$$W^A = \sum_{i=1}^N w_i^A P_i \quad \text{— for accessibility;}$$

$$W^{Au} = \sum_{i=1}^N w_i^{Au} P_i \quad \text{— for authenticity.}$$

Determination of the total threats for the safety components becomes:

$$W_{synerg}^{IB} = \sum_{i=1}^N (w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}) P_i, \quad \text{— for the part of IB;}$$

$$W_{synerg}^{KB} = \sum_{i=1}^N (w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}) P_i, \quad \text{— for component CS;}$$

$$W_{synerg}^{BI} = \sum_{i=1}^N (w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}) P_i, \quad \text{— a component for SI.}$$

Definition of generalized synergetic threats carried out in accordance with the expression (see Fig. 5.3):

$$W_{synerg}^{IS,CS,SI} = W_{synerg}^{IS} \cup W_{synerg}^{CS} \cup W_{synerg}^{SI}. \quad (5.8)$$

Definition of generalized synergetic threats based on their hybridity is determined by:

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

Obtained from the analysis of threats integration of data arriving at the 3rd level model of strategic management of the bank for their synthesis in assessing the adequacy of means of protecting BIn. The research results threat max th frequency BIn on their display in ABS are given in Table 5.2.

Table 5.2. — Results threat assessment based on a synergistic approach

Safety components	security services				
	$WITH, W_{synerg}^C$	I, W_{synerg}^I	A, W_{synerg}^I	Au, W_{synerg}^{Au}	Result
IB, W_{synerg}^{IB}	0.023	0.223	0.193	0.207	0.0002
KB, W_{synerg}^{KB}	0.222	0.234	0.197	0.134	0.0014
BI, W_{synerg}^{BI}	0.226	0.109	0.152	0.189	0.0007
Result	0.471	0.566	0.542	0.53	
$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \cup W_{synerg}^{KB} \cup W_{synerg}^{BI} =$ $= 0.0002 + 0.0014 + 0.0007 = \mathbf{0.0223}$					
$W_{synerg}^{hybrid\ C,I,A,Au} =$ $= W_{synerg}^C \cap W_{synerg}^I \cap W_{synerg}^A \cap W_{synerg}^{Au} =$ $= 0.471 \times 0.566 \times 0.542 \times 0.53 = \mathbf{0.0766}$					

Stage 2. Definition of generalized index of IB BIn in ABS. Based on the existing set of threats to information security, KBrB, BI on BIn in ABS and model hierarchy ABS — $G^{ABS} = \{\{O^{ABS}\}, \{L^{ABS}\}, \{I_A^{ABS}\}\}$ is determined by the relationship between information assets and threats to information security, KBrB, BI for the following actions:

- Determining the link between information assets BIn $\{I_A\}$ and elements of infrastructure ABS $A^{ABS} = \|a_{ij}^{ABS}\|$. Each element $I_{A_i} \in \{I_A\}$ described vector $I_{A_i} = (Type, A^C, A^I, A^A, A^{Au}, C_Y)$, *Type* — the type of information assets, described by the set of basic values *Type* = {BT, PID, CrD, KT, StO, Ol, YI, PD}, where BT — bank secrecy, PID — vouchers, CrD — credit instruments, KT — Commercial mystery, StO — statistical reports, Ol — public information, YI — control information, PD — personal data. A^C — confidentiality, A^I — integrity, A^A — availability, A^{Au} — authenticity, C_Y — continuity — the properties of information that must be provided. Takes values 1 — if the property is necessary, 0 — otherwise;

- Determine connection between information assets $\{I_A\}$ objects and environment. Each element $O_i \in \{O^{ABS}\}$ Described vector $O_i = \{Y^{ABS}, IO\}$, Where Y^{ABS} — level hierarchy information structure, defined by a plurality:

$Y^{ABS} = \{FL, NL, OSL, DBL, BL\}$, where FL — physical layer, NL — network level, OSL — level operating systems (OS), DBL — systems database management level, BL — level of banking technology applications and services. To specify the connection type and IO^R existing relationship between information assets and real environment using generally used:

$$IO^R = \|IO_{il}^R\|, \quad (5.9)$$

where IO_{il}^R — reflects the presence and type of connection between the i -th information assets and l -object of protection ABS.

Based on the proposed model synergetic threats:

$$GR^{ABS} = \{\{DF^{ABS}\}, \{T_{risk}\}, \{T_p\}, \{T_U\}, \{VH\}\}, \quad (5.10)$$

where $\{DF^{ABS}\}$ — set of threats, $\{T_{risk}\}$ — qualitative indicator of risk, $\{T_p\}$ — set basic terms probability of at least one threat j -th asset, $\{T_U\}$ — set basic terms value loss from the sale of threats, $\{VH\}$ — set conditions of destructive elements ABS and a generalized model of offender:

$$G_{IA}^{ABS} = \{aid_i, pur_i, T_{IA}, S_{\max_i}, pr_j, MS_i^{ABS}\} \forall i \in n, \forall j \in m, \quad (5.11)$$

where aid_i — ID offender (violator category), pur_i — the purpose of offender, T_{IA} — successful implementation of a threat, $S_{\max_i}$ — probabilistic damage system, pr_j — the likelihood of the realization of at least one threat j -th asset, MS_i^{ABS} — recommendations on detection, response TSZI performed for combining a plurality threats following:

$$DF^{ABS} = \{V^{NS}\} \cup \{V^{AS}\}, \text{ where } \{V^{AS}\} = \{V^{ASB1}\} \cap \{V^{ASIB}\} \cap \{V^{ASKB}\}. \quad (5.12)$$

This approach allows you to define the relationship between the sources of threats and elements of ABS $A^{DF} = \|a_{ij}^{DF}\|$ Protected.

Pricing full risk of all assets BIn:

$$R_{full} = \sum_{j=1}^n R_j, \quad (5.13)$$

where: $R_j = pr_j \times q_j$, where pr_j — probability of realization of at least one threat j -th asset;

q_j — loss.

The probability of realization of at least one threat to each asset BIn:

$$p_{rj} = 1 - \prod_{i=1}^m (1 - pr_{ij}), \quad (5.14)$$

where pr_{ij} — the probability of realization of the i -th threat j -th asset.

Definition of security threats ABS IS, CS, SI BIn to get the ABS is offered on the basis of the model:

$$G_{OZ}^{ABS} = \left\{ \begin{array}{l} \{I_A\}, \{O^{ABS}\}, \{DF^{ABS}\}, \{RR^{ABS}\}, \\ \{SZ^{ABS}\}, \{ROZ^{ABS}\}, \{UZ_r^{ABS}\} \end{array} \right\}, \quad (5.15)$$

where $\{I_A\}$ — the set of elements of information assets; $\{O^{ABS}\}$ — set elements hierarchy ABS; $\{DF^{ABS}\}$ — set of sources of security threats ABS; $\{RR^{ABS}\}$ — set requirements for security controls BIn; $\{SZ^{ABS}\}$ — set TSZI possible; $\{ROZ^{ABS}\}$ — accounting data on the results of security evaluations ABS; $\{UZ_r^{ABS}\}$ — the level of security of ABS.

Based on certain communications between the sources of threats and ABS elements defined relationship between threats and means of information security (TZSZI) — $A^{DFSZ} = \|a_{ij}^{DFSZ}\|$.

The model used the following types of communication: MZ — is a defense mechanism that provides the opposition to its destructive influence $VH_i \in \{VH\}$; NMZ — no protection mechanism to ensure the i -th counter threats.

If all $i = m$, $a_{mj}^{DFSZ} = NMZ$ Then concludes that TZSZI ABS can not protect BIn from this destructive influence and thus to increase the level of security of ABS must raise additional funds for protection mechanisms.

Defining the requirements of regulators $\{RR^{ABS}\}$ includes requirements for security BIn — $\{R_{BBI}\}$, defined in international and national standards set estimates the extent to which safety requirements $\{OV_{BBI}\}$ and set the final level of compliance with the safety requirements set BIn $\{R_{BBI}\}$, — $\{IU_{BBI}\}$:

$$\{RR^{ABS}\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}. \quad (5.16)$$

Generalized indicator of the level of security of ABS, to evaluate the level of compliance and regulatory requirements TZSZI determined:

$$OPZ^{ABS} = \sum_{i=1}^k OPZ_i, \quad (5.17)$$

where k — the number of private safety indicators, OPZ_i — private index takes values from the set: OPZ_i — no unacceptable risks, if in OPS in preparing models of threats/model of offender risk assessment found unacceptable to the level of risk is $OPZ_1 = 0$, otherwise — $OPZ_1 = 1$; OPZ_2 — no dangerous threats closure mechanisms TZSZI, $OPZ_2 = 0$, if the OPS in the preparation of a model

found “unbalanced” threat — $OPZ_2 = 1$; OPZ_3 — level security compliance requirements BIn regulators recommended recognized — $OPZ_3 = 1$, if deemed unauthorized — $OPZ_3 = 0$.

Stage 3. *Evaluation of effectiveness of investment in IB BIn in ABS.* Based on the generalized index of protection OPZ^{ABS} Generalized synergetic threat $W_{synerg}^{IB,KB,BI}$, A plurality of assets BIn $I_{A_i} = (Type, A^C, A^I, A^A, A^{Au}, C_Y)$ and the proposed model for evaluating investments in IB BIn in ABS on the state model of efficiency investments in OPS IB BIn that is different from known complexation economic indicators of investment in IB BIn in ABS considering synergy and hybridity attacks on security components, IB, CB, BI. Formally investment valuation model described by:

$$W_{ABS}^{effinv} = \left\{ I_{O^{ABS}}, \Delta^{ABS}, \{DF^{ABS}\}, rang^{ABS}, \{SZ^{ABS}\}, d^{ABS}, D^{ABS} \right\}, \quad (5.18)$$

$$\left\{ ROI^{ABS}, NPV^{ABS}, ROSI^{ABS}, r^{ABS}, CV^{ABS}, OU^{ABS} \right\},$$

where $I_{O^{ABS}}$ — the value of information assets; Δ^{ABS} — a sign of cost-effective-ness; $\{DF^{ABS}\}$ — set of sources of security threats BIn ABS; $rang^{ABS}$ — the cost of the development process TZZI; $\{SZ^{ABS}\}$ — set TZZI; d^{ABS} — present value of cash flow; ROI^{ABS} — rate of return on investment; NPV^{ABS} — the net present value; $ROSI^{ABS}$ — ROI TZZI; r^{ABS} — factor of profitability in the security BIn (SBIn); CV^{ABS} — the degree of risk per unit of average earnings; D^{ABS} — income from the use TZZI; OU^{ABS} — estimate the profit from the use TZZI.

State model of efficiency investments in IB BIn OPS (see Fig. 5.4):

Step 1. Evaluation of return on investment in information security:

$$ROI^{ABS} = NPV_{inv}^{ABS} - NPV_{zt}^{ABS}, \quad (5.19)$$

where: NPV_{inv}^{ABS} — Income from investments in TZZI ABS;

NPV_{zt}^{ABS} — Costs in TZZI ABS;

ROI^{ABS} — return on investments in TZZI ABS.

Step 2. Measuring return on investment in TZZI:

$$ROSI^{ABS} = NPV_{zbtshi}^{ABS} - NPV_{zvtszi}^{ABS}, \quad (5.20)$$

where: NPV_{zbtshi}^{ABS} — Costs of removal without the use of compromised security TZZI;

NPV_{zvtszi}^{ABS} — Costs of removal compromising safety using TZZI.

Step 3. Evaluation of net present value:

$$NPV_{zvtszi}^{ABS} = C_{sz} + \sum_{i=1}^N \frac{ALE_i}{(1+r)^i}, \quad (5.21)$$

where: N — number of intervals investments;

ALE_i — expected costs in the i -th period;

r — discount rate;

C_{sz} — cost remedies.

Step 4. BIn risk assessment methodology of calculation Annual loss expectancy — ALE , is the expected loss in each period of evaluation:

$$ALE^{ABS} = \sum_{i=1}^n I(O_{DF}^{ABS}) F_i, \quad (5.22)$$

where: $\{O_{DF}^{ABS}\}$ — set of threats;

$I(O_{DF}^{ABS})$ — cost implications of the threat;

ALE^{ABS} — the expected damage from the sale of threats;

F_i — Frequency (feature) of threats.

Step 5. Evaluation of potential losses U^{ABS} Information asset:

$$U^{ABS} = p_{rj} u_j, \quad (5.23)$$

where: p_{rj} — probability of realization of at least one threat j -th asset;

u_j — j -th value of the asset.

Step 6. Evaluation of total expected loss:

$$OU^{ABS} = \sum_{j=1}^n U^{ABS}. \quad (5.24)$$

The resulting data is fed to Level 1 model of strategic management of the bank for a decision on the status of IB Bin $S^{ABS} = \{S_1^{ABS}, S_2^{ABS}, \dots, S_m^{ABS}\}$.

Stage 4. Construction of integrated mechanisms to ensure the confidentiality, integrity, authenticity and credibility BIn in ABS. Based on assessments of the effectiveness TZZI the ABS to ensure confidentiality, integrity BIn proposed new mechanisms based on hybrid crypto-code designs on unprofitable codes (HCCDUC) that allow you to build asymmetric cryptosystem based on modified asymmetric crypto-code systems (MNCCS) McEliece with modified elliptical codes ((MEC) — short or long) to ensure an appropriate level of security and reliability BIn (see Fig. 5.4). Using unprofitable codes can reduce energy costs in the practical implementation MNCCS McEliece by reducing the power of the alphabet $GF(q)$, without reducing the overall resilience of cryptosystems in general and multi-use cryptography.

To modify elliptic code (MEA), which does not reduce the minimum distance of the code used to reduce its length by reducing the information symbols. $I = (I_1, I_2, \dots, I_k)$ — information vector (n, k, d) block code, a subset of h information symbols, $h = x$, $x \leq 1/2^k$ defines zero characters. When encoding information

symbols set vector h is not involved (they are zero) and can be discarded and the received codeword is shorter in x code symbols. The second method uses a modification increasing the length by forming initialization vector (defining symbols reduction) and replace null characters symbols vector information.

For damage using a universal mechanism of damage C_m :

$$\begin{aligned} CFT / CH_{FT} &= E_1(M, KU^{EC}), \\ CHD / CH_D &= E_2(M, KU^{EC}), \end{aligned} \quad (5.25)$$

$$M = E_{1,2}^{-1}(CFT / CH_{FT}, CHD / CH_D, KU^{EC}),$$

$$\text{where: } CFT / CH_{FT} = CFT / CH_{FT}^i, \dots, CFT / CH_{FT}^m,$$

$$KU^{EC} = \varphi(K_D^i, \dots, K_D^m, KU_1^{EC}, \dots, KU_m^{EC}),$$

$$CHD / CH_D = CHD / CH_D^i, \dots, CHD / CH_D^m.$$

Thus, the output ciphertext message (M) as a result of having two ciphertext (loss (CHD) and unprofitable text (FTC)), each of which alone can restore the original text.

The main properties are shown in Table MEA. 5.3 MNCCS main parameters in Table 5.4.

Protocols BIn in ABS using HCCDUC to shortened and elongated MEC codes shown in Fig. 5.5, 5.6, respectively.

Table 5.3. — Basic (n, k, d) MEC properties

Property	shortened MEC	MEC extended
(b, k, d) code options built through the reflection type $c: X \rightarrow P^{k-1}$	$n = 2\sqrt{q} + q + 1 - x,$ $k \geq \alpha - x, d \geq n - \alpha,$ $\alpha = 3 \times \deg F, k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1,$ $k \geq \alpha - x + x_1, d \geq n - \alpha,$ $\alpha = 3 \times \deg F$
(n, k, d) code options built through the reflection type $c: X \rightarrow P^{r-1}$	$n = 2\sqrt{q} + q + 1 - x,$ $k \geq n - \alpha, d \geq \alpha,$ $\alpha = 3 \times \deg F, k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1,$ $k \geq n - \alpha, d \geq \alpha,$ $\alpha = 3 \times \deg F$

Define Asymmetric crypto-code system with McElise EC [49, 51, 52, 53]: public key — the matrix: $G_X^{EC} = X \cdot G^{EC} \cdot P \cdot D$; private (secret) key — matrix X, P, D .

Cryptogram (kodohrama) — vector of length n : $c_X^* = i \cdot G_X^{EC} + e$,

where vector $c_X^* = i \cdot G_X^{EC}$ owned ES(n, k, d) — code with generative matrix G_X^{EC} , i — k -bit information vector, the vector e — secret weight vector error $\leq t$ (session key cryptosystems).

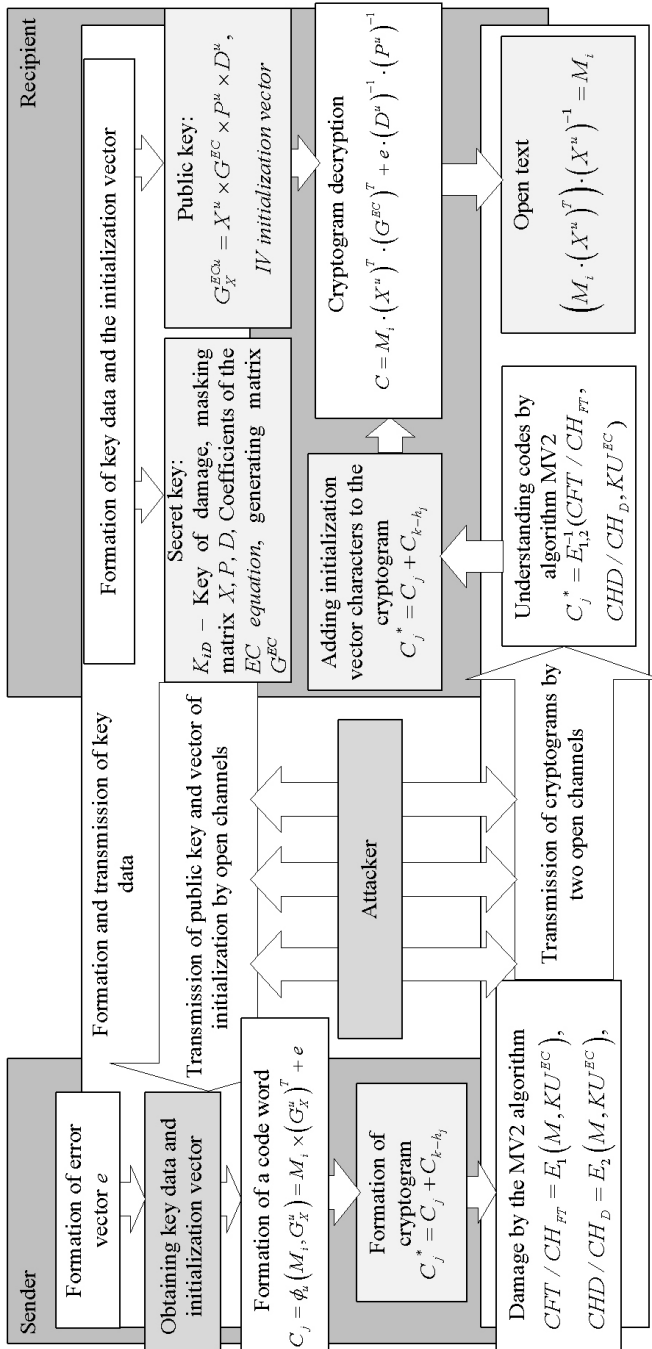


Fig. 5.5. Block diagram of the protocol confidentiality and integrity Bln in ABS based HCCDUC with short MEC

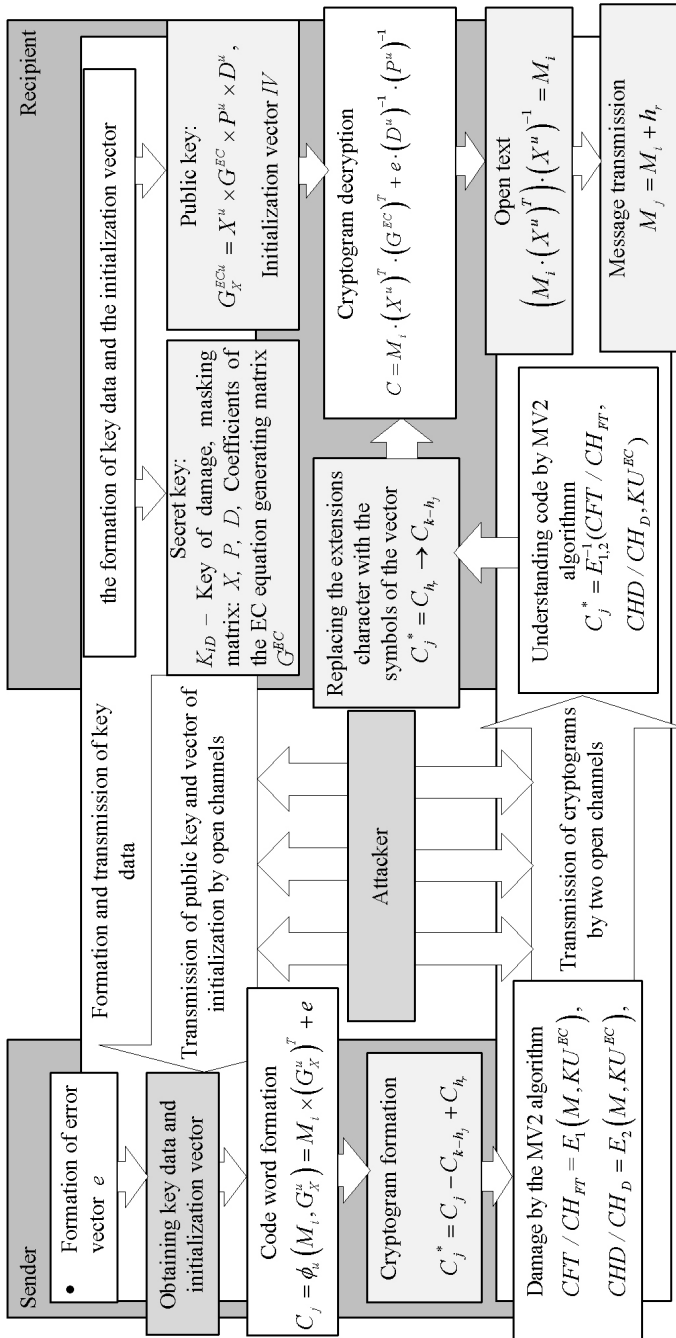


Fig. 5.6. Block diagram of the protocol confidentiality and integrity BIn in ABS based HCCDUC with extended MEC

Table 5.4. — The main parameters MNCCS McEliece at MEC

Property	shortened MEC	MEC extended
private key dimension	$l_{K+} = x \times \left\lceil \log_2(2\sqrt{q} + q + 1) \right\rceil$	$l_{K+} = (x - x_1) \times \log_2(2\sqrt{q} + q + 1)$
information vector dimension	$l_I = (\alpha - x) \times m$	$l_I = (\alpha - x + x_1) \times m$
cryptograms dimension	$l_S = (2\sqrt{q} + q + 1 - x) \times m$	$l_S = (2\sqrt{q} + q + 1 - x + x_1) \times m$
the relative speed	$R = \frac{(\alpha - x)}{(2\sqrt{q} + q + 1 - x)}$	$R = \frac{(\alpha - x + x_1)}{(2\sqrt{q} + q + 1 - x + x_1)}$

To ensure the authenticity of the BIn in ABS modified scheme is proposed to use two-factor authentication based on a password-OTP using HCCDUC on MNCCS McEliece and Niderraytera.

Define Asymmetric crypto-code system Niderraytera of the EU:

- public key — the matrix $G_X^{EC} = X \cdot G^{EC} \cdot P \cdot D$;
- private (secret) key — X, P, D matrix.

Cryptogram (kodohrama) — $c_X^* = i \cdot G_X^{EC} + e$, where vector $c_X^* = i \cdot G_X^{EC}$ owned EC (n, k, d) – code with generative matrix G_X^{EC} , i – k -bit information vector, the vector e – secret weight vector error $\leq t$ (session key cryptosystems).

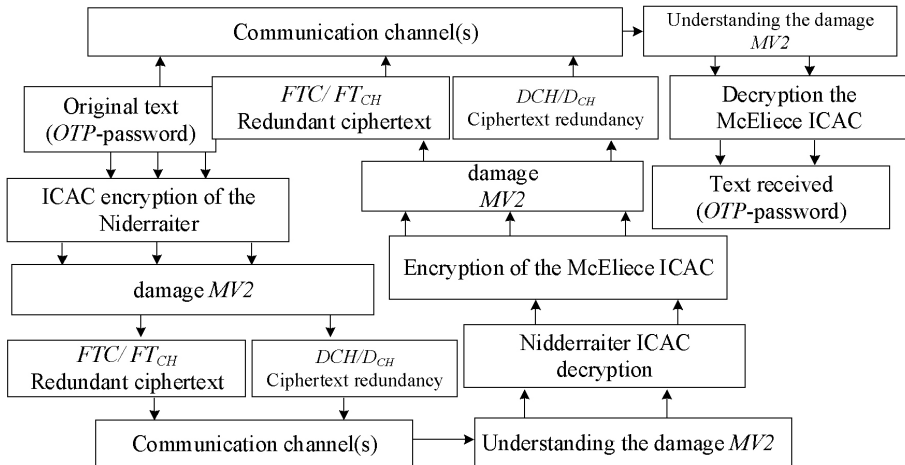


Fig. 5.7. Block diagram of the protocol improved method of OTP-based authentication HCCDUC

Block diagram of the protocol improved method of OTP-based authentication HCCDUC shown in Fig. 5.7 [60].

The use of hybrid crypto-code designs on unprofitable codes can increase the number of token authenticator, use two asymmetric crypto-code system, two/four channels unprofitable text authenticator and loss. Scalable software module by changing the parameters MNCCS Niderraytera and/or McEliece, depending on the requirements put forward a communication channel ABS ensures its implementation in mobile gadgets and compatibility with the protocols used to transmit data to the Internet and mobile networks.

Stage 5. *Defining the strategies and formation of IB BIn in ABS.* At the final stage of a three-tier strategy implemented safety management BIn in ABS (see Fig. 5.4).

First level describes the overall corporate strategy of the bank and its functional strategy. Corporate strategy defines development prospects and serves the core mission of the bank. At this level, according to a synergistic approach. The general concept of security of information technology ABS and emerging goals and objectives to ensure KBrB. This level is determined by the state of IB BIn in ABS: $S^{ABS} = \{S_1^{ABS}, S_2^{ABS}, ..., S_m^{ABS}\}$.

Functional strategies are one of horizontal communication and coordinated at the level of goals, with further detail at the next level strategic set.

The second level is formed corporate strategy IS BIn in ABS:

$$\{RR^{ABS}\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}.$$

Defined goals and objectives of key business processes relating to the protection of personal data of legal and private clients. Corporate Security Strategy describes how you want to manage and coordinate the efforts of various aspects of security. It develops functional strategies, economic financial, physical and information security.

The third level is made functional strategies detailed second-level strategic set formed corporate security strategy information. The main areas to protect advisable to provide personnel security, physical security, network and BI. At this level, determined in accordance with applicable TZSZI between IS and threats, CS, SI BIn on the ABS — $OPZ^{ABS} = \sum_{i=1}^k OPZ_i$. IB strategy is an important function of the bank's management and security should be formed and held senior management.

The concept of strategic IT security management ABS Ukraine-based three-tier model and synergetic model threats against known covers all main areas of the bank's activities to ensure information security. This concept is based

on a synergistic approach to the selection of the most effective ways achieving goals IS BIn in ABS to the value of risk at every level model of strategic management of the bank. The approach allows to conduct comprehensive selection of possible alternatives strategic decisions on security issues.

The proposed methodology for constructing systems for IS BIn in ABS unlike known approaches implements a radically new concept hybrid countering threats to the banking sector. Its essence and meaning is the rational organization of information security software BIn in ABS in terms of simultaneous action on the system of information security threats, kiberbezpetsi and safety information. The methodology is based on a model first proposed three-level strategic security management of information technology in ABS. Its basis is first introduced synergetic model of information security threats banking information that allowed to generalize the model known offender security of banking information. On the basis of the methodology was developed classifier information security threats in part, concerning the simultaneous consideration of it except threats information security threats and security risks kiberbezpetsi data bank information in the ABS. Implementation Branch led to the conclusion that the hybrid to counter threats to banking information ABS advisable to use new mechanisms to ensure integrated services based on HCCDUC who also designed according to the proposed methodology.

The proposed HCCDUC based on cryptographic transformations and unprofitable noise-coding, allowing security services to ensure their probability for a given performance. So speed crypto-conversion provided at BSC, cryptographic strength at 10^{25} – 10^{35} batch operations, the reliability of transfer banking information in ABS open communication channels not below $P_{\text{error}} 10^{-9}$ – 10^{-12} .

The submitted methodology is an effective tool for developing practical applications as software and firmware that implements a certain system for IB BIn in ABS security policy. Practical methodology indication confirmed by relevant acts introduction of leading banks in Ukraine.

5.3 Experiment

The experiment was carried out in compliance with the essential requirements that apply to his conduct, namely a plan of the experiment, and experiment program The analysis of the results.

Let us consider certain points.

To plan the experiment included:

1. purpose of the experiment;
2. tasks experiment;
3. Justification of the choice sets threats BIn in ABS.

The aim of the experiment is check the adequacy of methods of evaluating the effectiveness of functioning ABS composite indicator based assessment of quality of service objects on automated banking system selection of alternatives possible strategic decisions on security issues. The object of the study determined the threat to the safety components: IS, CS, SI BIn in ABS, which ensures minimization of investment in building a BI system IS ABS.

The main objectives of the experiment, the following:

- determine the probability of the impact of threats IS, CS, SI BIn;
- determining relationships between elements of infrastructure ABS information assets BIn, threats IS, CS, SI and TZZI improved model based infrastructure ABS synergetic model threats, improved model of the attacker;
- definition of generalized index of IB BIn in ABS based on improved model of evaluation of the security BIn in ABS;
- evaluating investment in IB BIn in ABS, which differs from the known complexation economic indicators of investment in IB BIn in ABS considering synergy and hybridity attacks on security components, IB, CB, BI;
- the adequacy of the study methods of evaluating the effectiveness of ABS operation through integrated assessment indicator of quality of service objects on automated banking system selection of alternatives possible strategic decisions on security issues.

Rationale selecting a plurality of threats BIn in ABS. Applying the developed methodology of constructing a system of information security of banking information in automated banking systems (see Fig. 5.3, 5.4) as the set of threats BIn in ABS with threats choose Web resource (<http://bdu.fstec.ru/threat>) [61] Fig. 5.8.

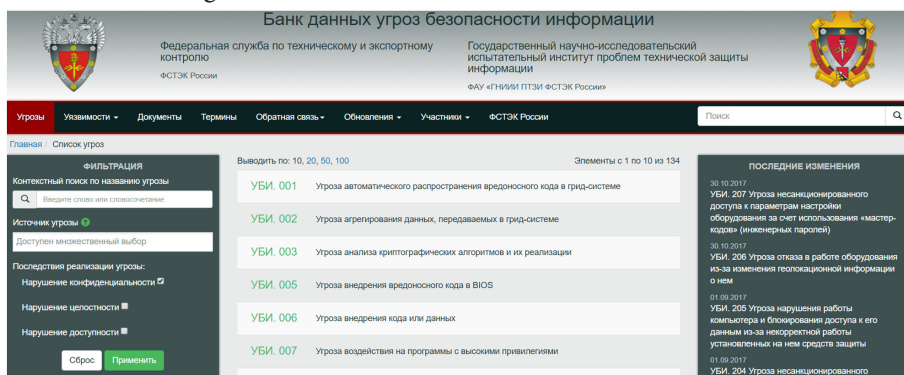


Fig. 5.8. Choosing a plurality threats resource “Data Bank information security threats”

The software resource experiment regulates the procedure for organizing and conducting:

Stage 1. *Determining the impact probability of threats IB, CB, BI information security BIn:*

Step 1. Forming metric coefficients experts threats for security services:

$$d_i = \Pi(M_{ih}^{DFABS})^{w_{ih}^{DFABS}}, \quad (5.26)$$

where: M_{ih}^{DFABS} — the value of h -th metric of i -offender;

w_{ih}^{DFABS} — weight h -th metric of i -offender $\sum_h w_{ih}^{DFABS} = 1$.

Fig. 5.9 shows the construction of metric weight data for components of security services all threats to information resources in a BIn in the ABS software resources (<http://skl.hneu.edu.ua>).

Fig. 5.9. Formation metric coefficients experts threats

Based introduced metrics calculated performance metrics main threats: mathematical custody — μ i -th threats $i \in [1; N]$, where N — number of threats on classifier variance — σ i -th threats $i \in [1; N]$. In the calculations take into account the possibility classifier dependent threats (threats codes match), then the first is full probability dependent on threats and calculated key figures for independent threats. Appendix E shows the results of the study threats to information security of banking information in automated banking systems based on the proposed classifier (Fig. 5.10–5.13).

Step 1.2 Forming identifiers threats on classifier components. Classifier components are:

- security component BIn in OPS ABS: IS (01), SI (02), CS (03);
- the nature areas: regulatory (01), organizational (02), engineering (03);
- the main features of information: privacy (01), integrity (02), availability (03), authenticity (04);
- the hierarchy of infrastructure ABS: FL — physical layer (01), NL — network layer (02), OSL — level operating systems (OS) (03), DBL — level database management systems (04), BL — level banking technology applications and services (05) (Fig. 5.10).

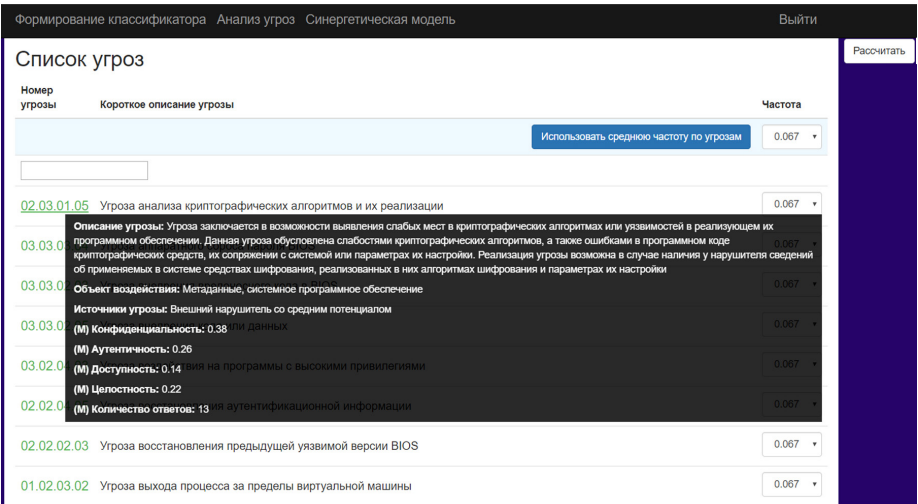


Fig. 5.10. Formation classifier by components

Step 1.3 Determine the probability of occurrence P_i i -th threats (table 5.5) (Fig. 5.11). Suggested value occurrence probability P_i i -th based on threat experts metrics for each component of the security services, with the result ranking.

Table 5.5. — Table determine the potential threats, depending on the frequency of their manifestation

P_i	The incidence of threats
0.067	threat appears no more than once every 5 years
0.133	threat appears no more than once a year
0.2	threat appears no more than once a month
0.267	threat appears no more than once a week
0.333	threat manifests itself daily

Fig. 5.11. Identifying the potential threats, depending on the frequency of their manifestation

$$w_i = w^C_i P_i \cup w^I_i P_i \cup w^A_i P_i \cup w^{Au}_i, P_i = 1, \quad (5.27)$$

where $w_i^C, w_i^I, w_i^A, w_i^{Au}$ — expert weights security services: confidentiality, integrity, availability, authenticity, P_i — probability of the i -th threats (Fig. 5.12).

Fig. 5.12. Rezultaty assessment of key indicators for each threat (μ, σ)

Step 1.5 Determining the likelihood of multiple threats at specified security service determined by the expression (5.27):

$$W_{synerg}^C = \sum_{i=1}^M w_i^C \alpha_i^C = 0.009 + 0.142 + 0.099 = 0.25 \text{ — service privacy;}$$

$$W_{synerg}^I = \sum_{i=1}^M w_i^I \alpha_i^I = 0.112 + 0.155 + 0.061 = 0.328 \text{ — service integrity;}$$

$$W_{synerg}^A = \sum_{i=1}^M w_i^A \alpha_i^A = 0.108 + 0.123 + 0.088 = 0.319 \text{ — service availability;}$$

$$W_{synerg}^{Au} = \sum_{i=1}^M w_i^{Au} \alpha_i^{Au} = 0.126 + 0.047 + 0.141 = 0.314 \text{ — the authenticity of}$$

the service (5.9), where N — total number of threats in the classifier.

Step 1.6 Determination of the total threats for the security components based expression (2) is determined by:

$$\begin{aligned} W_{synerg}^{IS} &= \sum_{i=1}^N (w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}) P_i = \\ &= 0.009 \times 0.112 \times 0.108 \times 0.126 = 0.0000137, \end{aligned}$$

$$\begin{aligned} W_{synerg}^{CS} &= \sum_{i=1}^N (w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}) P_i = \\ &= 0.142 \times 0.155 \times 0.123 \times 0.047 = 0.0001272, \end{aligned}$$

$$\begin{aligned} W_{synerg}^{SI} &= \sum_{i=1}^N (w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}) P_i = \\ &= 0.099 \times 0.061 \times 0.088 \times 0.141 = 0.0000749. \end{aligned}$$

Table 5.6. — Results threat assessment based on a synergistic approach

safety compo- nents	security services				
	$WITH, W_{synerg}^C$	I, W_{synerg}^I	A, W_{synerg}^A	Au, W_{synerg}^{Au}	Result
IS, W_{synerg}^{IB}	0.023	0.223	0.193	0.207	0.0002
CS, W_{synerg}^{KB}	0.222	0.234	0.197	0.134	0.0014
SI, W_{synerg}^{BI}	0,226	0,109	0.152	0.189	0.0007
Result	0.471	0.566	0.542	0.53	
$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \cup W_{synerg}^{KB} \cup W_{synerg}^{BI} =$ $= 0.0002 + 0.0014 + 0.0007 = 0.00223$			$W_{synerg}^{hybrid\ C,I,A,Au} =$ $= W_{synerg}^C \cap W_{synerg}^I \cap W_{synerg}^A \cap W_{synerg}^{Au} =$ $= 0.471 \times 0.566 \times 0.542 \times 0.53 = 0.0766$		

Stage 1.7 Definition of generalized synergetic threats in the BIn ABS:

$$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \cup W_{synerg}^{KB} \cup W_{synerg}^{BI} = 0.0002 + 0.0014 + 0.0007 = \mathbf{0.000216}. \quad (5.28)$$

Stage 1.8 Definition of generalized synergetic threats based on their hybridity is determined (Fig. 5.13, Table 5.6):

$$W_{synerg}^{hybrid\ C,I,A,Au} = W_{synerg}^C \cap W_{synerg}^I \cap W_{synerg}^A \cap W_{synerg}^{Au} = 0.471 \times 0.566 \times 0.542 \times 0.53 = \mathbf{0.008214}. \quad (5.29)$$

Формирование классификатора Анализ угроз Синергетическая модель								Выйти
03.01.01.01	Угроза подключения к беспроводной сети в обход процедуры аутентификации							0.009 0.044 0.013 0.066 0.246 0.022 0.063 0.269
03.01.04.01	Угроза подмены беспроводного клиента или точки доступа							0 0.067 0.067 0.134 0.312 0.012 0.23 0.043

Составные безопасности	Услуги безопасности				
	C, W_{synerg}^C	I, W_{synerg}^I	A, W_{synerg}^A	Au, W_{synerg}^{Au}	Итого
01 - IB, W_{synerg}^{IB}	0.009	0.112	0.108	0.126	0.0000137
02 - KB/B, W_{synerg}^{KB+B}	0.142	0.155	0.123	0.047	0.0001272
03 - BI, W_{synerg}^{BI}	0.099	0.061	0.088	0.141	0.0000749
Итого	0.25	0.328	0.319	0.314	
$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \cup W_{synerg}^{KB+B} \cup W_{synerg}^{BI} = 0.000216$					
$W_{synerg}^{hybrid\ C,I,A,Au} = W_{synerg}^C \cap W_{synerg}^I \cap W_{synerg}^A \cap W_{synerg}^{Au} = 0.008214$					

© 2017 - Угрозы безопасности информации

Fig. 5.13. Results threat assessment based on a synergistic approach

Stage 2. Defining relationships between elements of infrastructure ABS information assets BIn, threats IS, CS, SI and TZZI improved model based infrastructure ABS synergetic model threats, improved model attacker:

Based on the existing set of threats IS, CS, SI BIn on the ABS and ABS model hierarchy — $G^{ABS} = \{\{O^{ABS}\}, \{L^{ABS}\}, \{I_A^{ABS}\}\}$, where $\{O^{ABS}\}$ — set of objects environment ABS descriBing elements ABS and they belong to levels of hierarchy ABS, $\{L^{ABS}\}$ — set of links between elements of ABS, $\{I_A^{ABS}\}$ — set of information assets BIn (see subsection 2.3.1, Fig. 5.14).

Step 2.1 Determining the link between BIn information assets $\{I_A\}$ and elements of infrastructure ABS $A^{ABS} = \|\alpha_{ij}^{ABS}\|$. Each element $I_{A_i} \in \{I_A\}$ described vector $I_{A_i} = (Type, A^C, A^I, A^A, A^{Au}, C_Y)$, *Type* — the type of information assets, described by the set of basic values $Type = \{BT, PID, CrD, KT, StO, Ol, YI, PD\}$, where *BT* — bank secrecy, *PID* — vouchers, *CrD* — credit instruments, *KT* — Commercial mystery, *StO* — statistical reports, *Ol* — public information, *YI* —

control information, PD — personal data. A^C — confidentiality, A^I — integrity, A^A — availability, A^{Au} — authenticity, C_y — continuity — the properties of information that must be provided. Takes values 1 — if the property is necessary, 0 — otherwise (Fig. 5.14).

Формирование классификатора Анализ угроз Синергетическая модель Выйти

	C	I	A	Au
Банковская тайна	1 ▾	1 ▾	1 ▾	1 ▾
Платежные документы	1 ▾	1 ▾	1 ▾	1 ▾
Кредитные документы	1 ▾	1 ▾	1 ▾	1 ▾
Коммерческая тайна	1 ▾	1 ▾	1 ▾	1 ▾
Статистические отчеты	0 ▾	1 ▾	1 ▾	1 ▾
Общедоступная информация	0 ▾	1 ▾	1 ▾	0 ▾
Управляющая информация	0 ▾	1 ▾	1 ▾	1 ▾
Персональные данные	1 ▾	1 ▾	1 ▾	1 ▾

0 - услуга не обеспечивается.
1 - услуга обеспечивается.

Следующий шаг

	Физ. уровень	Сетевой уровень	Уровень ОС	Уровень СУБД	Уровень банковского ПО
Банковская тайна	p ▾	p ▾	s ▾	c ▾	so ▾
Платежные документы	p ▾	p ▾	s ▾	c ▾	so ▾
Кредитные документы	p ▾	p ▾	s ▾	c ▾	so ▾
Коммерческая тайна	p ▾	p ▾	s ▾	c ▾	so ▾
Статистические отчеты	p ▾	p ▾	s ▾	c ▾	so ▾
Общедоступная информация	p ▾	p ▾	s ▾	c ▾	so ▾
Управляющая информация	p ▾	p ▾	s ▾	c ▾	so ▾
Персональные данные	p ▾	p ▾	s ▾	c ▾	so ▾

0 - связь отсутствует - 0;
cs - включает и хранит - 0.5;
pt - обрабатывает или передает - 0.22;
so - поддерживает функционирование - 0.17;

© 2017 - Угрозы безопасности информации

Fig. 5.14. Defining the relationship between information assets Bln, security services and advanced infrastructure elements ABS

Step 2.2 Inyznachennya connection between information assets $\{I_A\}$ objects and environments (Fig. 5.14, Table 5.7, 5.8). Each element $O_i \in \{O^{ABS}\}$ Described vector $O_i = \{Y^{ABS}, IO\}$, where Y^{ABS} — level hierarchy information structure, defined by a plurality $Y^{ABS} = \{FL, NL, OSL, DBL, BL\}$, where FL — physical layer, NL — network level, OSL — operating systems (OS) level, DBL — level of systems database management, BL — level of banking technology applications and services. To specify the connection type and IO^R existing relationship between information assets and real environment using generally used:

$$IO^R = \|IO_{il}^R\|, \quad (5.30)$$

where IO_{il}^R — reflects the presence and type of connection between the i -th information assets and l -object of ABS environment.

In this $\forall i \in \{I_A\}$, a $\forall l \in \{O^{ABS}\}$:

$$IO_{il}^R = \begin{cases} 0, & \text{connection is absent;} \\ cs, & \text{includes and retains;} \\ pt, & \text{processes or transfers;} \\ so, & \text{keeps functioning.} \end{cases} \quad (5.31)$$

Each parameter is assigned weight classes Fishburne rule [65], based on the fact that change is subject to criteria weighting coefficients descending arithmetic progression.

In this first criterion ($i=1$), is the first in a strictly ordered by importance criteria ranked number $i=1, 2, \dots, n$, is the most important and has the greatest weight. This rule is given by the expression:

$$w_i = \frac{2(N-n+1)}{N(N+1)}, \quad (5.32)$$

where: w_i – weight Fishburne;

N – the total number of parameters;

n – serial number parameter;

i – number of parameters.

According to the expression Fishburne have:

$$w_1 = \frac{2 \times N}{N(N+1)}, \quad w_N = \frac{2}{N(N+1)}, \quad \gamma = \frac{w_1}{w_N} = N, \quad (5.33)$$

where γ – the multiplicity of weighting coefficients differences from each other.

So, $cs = 0.5$, $pt = 0.22$, $so = 0.17$.

Step 2.3 Definition of integration sets threats based threats synergetic model and generalized model of the offender.

Synergetic Model threats formally described by:

$$GR^{ABS} = \{\{DF^{ABS}\}, \{T_{risk}\}, \{T_P\}, \{T_U\}, \{VH\}\}, \quad (5.34)$$

where: $\{DF^{ABS}\}$ – set of threats;

$\{T_{risk}\}$ – qualitative indicator of risk;

$\{T_P\}$ – set basic terms probability of at least one threat j -th asset;

$\{T_U\}$ – set basic terms value loss from the sale of threats;

$\{VH\}$ – set conditions of destructive elements ABS.

Table 5.7. — Service delivery information assets Bln in ABS

Name, I_{A_i}	<i>WITH</i>	<i>I</i>	<i>A</i>	<i>Au</i>
<i>BT</i>	1	1	1	1
<i>PID</i>	1	1	1	1
<i>CrD</i>	1	1	1	1
<i>KT</i>	1	1	1	1
<i>StO</i>	0	1	1	1
<i>Ol</i>	0	1	1	0
<i>YI</i>	0	1	1	1
<i>PD</i>	1	1	1	1

Table 5.8. — Relationship information assets Bln with elements of a generalized infrastructure ABS

Name, I_{A_i}	Physical Layer	Network Layer	level OS	level data-base	Level Bank-ing Software
<i>BT</i>	Pt	Pt	so	cs	so
<i>PID</i>	Pt	Pt	so	cs	so
<i>CrD</i>	Pt	Pt	so	cs	so
<i>KT</i>	Pt	Pt	so	cs	so
<i>StO</i>	Pt	Pt	so	cs	so
<i>Ol</i>	Pt	Pt	so	cs	so
<i>YI</i>	Pt	Pt	so	cs	so
<i>PD</i>	Pt	Pt	so	cs	so

Generalized model identified five categories of offender and formally described by:

$$G_{LA}^{ABS} = \{aid_i, pur_i, T_{LA}, S_{\max_i}, pr_j, MS_i^{ABS}\} \forall i \in n, \forall j \in m, \quad (5.35)$$

where aid_i — ID offender (violation category); pur_i — the purpose of offender; T_{LA} — successful implementation of a threat; $S_{\max_i}$ — probabilistic damage system; pr_j — the likelihood of the realization of at least one threat j -th asset; MS_i^{ABS} — recommendations on detection, response TSZI.

Based on the proposed models for combining a plurality of threats made (Fig. 5.33, Table 5.9):

$$DF^{ABS} = \{V^{NS}\} \cup \{V^{AS}\},$$

where $\{V^{AS}\} = \{V^{ASIB}\} \cap \{V^{ASKB}\} \cap \{V^{ASBI}\}$, where $\{V^{NS}\}$ — class natural sources of threats; $\{V^{AS}\}$ — Class anthropogenic threats where; $\{V^{ASIB}\}$ — set of

threats to information security; $\{V^{ASKB}\}$ — set of cyber security threats; $\{V^{ASBI}\}$ — set BI threats.

Table 5.9. — Determining the probability of at least one threat to each asset Bln

ID of threats	BT	PID	CrD	KT	StO	Ol	YI	PD
02.03.01.05	0.268	0.268	0.268	0.268	0.241	0.153	0.241	0.268
03.03.03.04	0.332	0.332	0.332	0.332	0.166	0.066	0.166	0.332
03.03.02.03	0.332	0.332	0.332	0.332	0.249	0.166	0.249	0.332
03.03.02.05	0.333	0.333	0.333	0.333	0.223	0.113	0.223	0.333
03.02.04.03	0.332	0.332	0.332	0.332	0.222	0.189	0.222	0.332
02.02.04.05	0.268	0.268	0.268	0.268	0.18	0.046	0.18	0.268
02.02.02.03	0.2	0.2	0.2	0.2	0.1	0.05	0.1	0.2
01.02.03.02	0.268	0.268	0.268	0.268	0.134	0.107	0.134	0.268
03.02.03.01	0.267	0.267	0.267	0.267	0.23	0.203	0.23	0.267
03.02.02.03	0.268	0.268	0.268	0.268	0.241	0.222	0.241	0.268
...	...	...	...	...	...	...	...	...
03.03.02.03	0.267	0.267	0.267	0.267	0.2	0.112	0.2	0.267
01.01.03.05	0.133	0.133	0.133	0.133	0.114	0.101	0.114	0.133
03.03.02.04	0.332	0.332	0.332	0.332	0.199	0.116	0.199	0.332
03.01.03.02	0.267	0.267	0.267	0.267	0.182	0.094	0.182	0.267
01.01.03.04	0.332	0.332	0.332	0.332	0.299	0.189	0.299	0.332
03.01.01.01	0.2	0.2	0.2	0.2	0.186	0.086	0.186	0.2
03.01.04.01	0.132	0.132	0.132	0.132	0.132	0.066	0.132	0.132
03.01.04.05	0.268	0.268	0.268	0.268	0.249	0.115	0.249	0.268
03.01.04.05	0.268	0.268	0.268	0.268	0.228	0.094	0.228	0.268

Step 2.4 Definitionfull price of risk assets Bln (see Table. 5.6):

$$R_{povm} = \sum_{j=1}^n R_j, \quad (5.38)$$

where: $R_j = pr_j \times q_j$,

where: pr_j — probability of realization of at least one threat j -th asset;
 q_j — loss.

Step 2.5 Determining the probability of at least one threat to each asset Bln (Fig. 5.15, Table 5.34):

$$p_{rj} = 1 - \prod_{i=1}^m (1 - pr_{ij}), \quad (5.39)$$

where: pr_{ij} — the probability of realization of the i -th threat j -th asset.

Формирование классификатора Анализ угроз Синергетическая модель								Выйти
Синергитическая модель.								
	Банковская тайна	Платежные документы	Кредитные документы	Коммерческая тайна	Статистические отчеты	Общедоступная информация	Управляющая информация	Персональные данные
02.03.01.05	0.268	0.268	0.268	0.268	0.241	0.153	0.241	0.268
03.03.03.04	0.332	0.332	0.332	0.332	0.166	0.066	0.166	0.332
03.03.02.03	0.999	0.999	0.999	0.999	0.733	0.43	0.733	0.999
03.03.02.05	0.5777	0.5777	0.5777	0.5777	0.4277	0.2394	0.4277	0.5777
03.02.04.03	0.5176	0.5176	0.5176	0.5176	0.3631	0.2663	0.3631	0.5176
02.02.04.05	0.268	0.268	0.268	0.268	0.18	0.046	0.18	0.268
02.02.02.03	0.2	0.2	0.2	0.2	0.1	0.05	0.1	0.2
01.02.03.02	0.268	0.268	0.268	0.268	0.134	0.107	0.134	0.268
03.02.03.01	0.3294	0.3294	0.3294	0.3294	0.2712	0.2335	0.2712	0.3294
03.02.02.03	0.268	0.268	0.268	0.268	0.241	0.222	0.241	0.268
01.01.03.05	0.666	0.666	0.666	0.666	0.56	0.421	0.56	0.666
03.03.02.04	0.4433	0.4433	0.4433	0.4433	0.2722	0.1589	0.2722	0.4433
03.01.03.02	0.5791	0.5791	0.5791	0.5791	0.4639	0.2756	0.4639	0.5791
01.01.03.04	0.5178	0.5178	0.5178	0.5178	0.4364	0.2819	0.4364	0.5178
03.03.03.03	0.6654	0.6654	0.6654	0.6654	0.4895	0.2857	0.4895	0.6654
02.03.01.02	0.5735	0.5735	0.5735	0.5735	0.2849	0.154	0.2849	0.5735
01.01.02.05	0.6653	0.6653	0.6653	0.6653	0.5533	0.3446	0.5533	0.6653

Fig. 5.15. Probability of i -th threats to information assets Bln in ABS

Step 2.6 *Determining the link between the sources of threats and elements of ABS (Fig. 5.16, Table 5.10):*

$$A^{DF} = \|a_{ij}^{DF}\|. \quad (5.36)$$

Формирование классификатора Анализ угроз Синергетическая модель					Выйти
	Физический уровень	Сетевой уровень	Уровень операционных систем	управления базами данных	технологических приложений и сервисов
02.03.01.05	0.4345	0.4345	0.33575	0.9875	0.33575
03.03.03.04	0.45276	0.45276	0.34986	1	0.34986
03.03.02.03	0.51128	0.51128	0.39508	1	0.39508
03.03.02.05	0.48928	0.48928	0.37808	1	0.37808
03.02.04.03	0.50446	0.50446	0.38981	1	0.38981
02.02.04.05	0.38412	0.38412	0.29682	0.873	0.29682
02.02.02.03	0.275	0.275	0.2125	0.625	0.2125
01.02.03.02	0.3773	0.3773	0.29155	0.8575	0.29155
03.02.03.01	0.43956	0.43956	0.33966	0.999	0.33966
03.02.02.03	0.44968	0.44968	0.34748	1	0.34748
03.03.02.03	0.40634	0.40634	0.31399	0.9235	0.31399
01.01.03.05	0.21868	0.21868	0.16898	0.497	0.16898
03.03.02.04	0.47828	0.47828	0.36958	1	0.36958
03.01.03.02	0.39446	0.39446	0.30481	0.8965	0.30481
01.01.03.04	0.53834	0.53834	0.41599	1	0.41599
03.03.03.03	0.48928	0.48928	0.37808	1	0.37808

Fig. 5.16. Determining the link between the sources of threats and elements of ABS

Table 5.10. — Determining the link between the sources of threats and elements of ABS

ID threats	Physical Layer	Network Layer	level OS	level database	Level Banking Software
02.03.01.05	0.4345	0.4345	0.33575	0.9875	0.33575
03.03.03.04	0.45276	0.45276	0.34986	1	0.34986
03.03.02.03	0.51128	0.51128	0.39508	1	0.39508
03.03.02.05	0.48928	0.48928	0.37808	1	0.37808
03.02.04.03	0.50446	0.50446	0.38981	1	0.38981
...	...	...	...	...	...
03.01.01.01	0.32076	0.32076	0.24786	0.729	0.24786
03.01.04.01	0.2178	0.2178	0.1683	0.495	0.1683
03.01.04.05	0.42966	0.42966	0.33201	0.9765	0.33201
03.01.04.05	0.4158	0.4158	0.3213	0.945	0.3213
02.03.02.03	0.28512	0.28512	0.22032	0.648	0.22032
03.02.03.01	0.10098	0.10098	0.07803	0.2295	0.07803

Stage 3. Definition of generalized index of IB BIn in ABS based on improved model of evaluation of the security BIn in ABS.

Definition of security threats ABS IB, CB, BI BIn to get the ABS is offered on the basis of the model:

$$G_{OZ}^{ABS} = \left\{ \begin{array}{l} \{I_A\}, \{O^{ABS}\}, \{DF^{ABS}\}, \{RR^{ABS}\}, \\ \{SZ^{ABS}\}, \{ROZ^{ABS}\}, \{UZ_r^{ABS}\} \end{array} \right\}, \quad (5.39)$$

where: $\{I_A\}$ — the set of elements of information assets;

$\{O^{ABS}\}$ — set elements hierarchy ABS;

$\{DF^{ABS}\}$ — set of sources of security threats ABS;

$\{RR^{ABS}\}$ — set requirements for security controls BIn;

$\{SZ^{ABS}\}$ — set TSZI possible;

$\{ROZ^{ABS}\}$ — accounting data on the results of security evaluations ABS;

$\{UZ_r^{ABS}\}$ — the level of security of ABS.

Step 3.1 Determining the link between threats and means of information security (TZZI) (Fig. 5.17, Table 5.11):

$$A^{DFSZ} = \|a_{ij}^{DFSZ}\|, \text{ with } \forall j \in \{I_A\} \text{ and } \forall i \in \{DF_i\}. \quad (5.40)$$

Формирование классификатора Анализ угроз Синергитическая модель Выйти

Синергитическая модель.

MZ - механизм защиты, обеспечивает противодействие ее деструктивному влиянию.
NMZ - нет механизма защиты для обеспечения противодействия i-той угрозы;

	Физический уровень	Сетевой уровень	Уровень операционных систем	Уровень систем управления базами данных	Уровень банковских технологических приложений и сервисов
02.03.01.05	MZ	MZ	MZ	MZ	MZ
03.03.03.04	MZ	MZ	MZ	MZ	MZ
03.03.02.03	MZ	MZ	MZ	MZ	MZ
03.03.02.05	MZ	MZ	MZ	MZ	MZ
03.02.04.03	MZ	MZ	MZ	MZ	MZ
02.02.04.05	MZ	MZ	MZ	MZ	MZ
02.02.02.03	MZ	MZ	MZ	MZ	MZ
01.02.03.02	MZ	MZ	MZ	MZ	MZ
03.02.03.01	MZ	MZ	MZ	MZ	MZ
03.02.02.03	MZ	MZ	MZ	MZ	MZ
03.03.02.03	MZ	MZ	MZ	MZ	MZ
01.01.03.05	MZ	MZ	MZ	MZ	MZ

Fig. 5.17. The relationship between threats and TZZI

Table 5.11. — The relationship between threats and TZZI

ID threats	Physical Layer	Network Layer	level OS	level database	Level Banking Software
02.03.01.05	MZ	MZ	MZ	MZ	MZ
03.03.03.04	MZ	MZ	MZ	MZ	MZ
03.03.02.03	MZ	MZ	MZ	MZ	MZ
03.03.02.05	MZ	MZ	MZ	MZ	MZ
03.02.04.03	MZ	MZ	MZ	MZ	MZ
...	...	...	...	...	...
03.01.01.01	MZ	MZ	MZ	MZ	MZ
03.01.04.01	MZ	MZ	MZ	MZ	MZ
03.01.04.05	MZ	MZ	MZ	MZ	MZ
03.01.04.05	MZ	MZ	MZ	MZ	MZ
02.03.02.03	MZ	MZ	MZ	MZ	MZ
03.02.03.01	MZ	MZ	MZ	MZ	MZ

The model used the following types of communication: MZ — is a defense mechanism that provides the opposition to its destructive influence $VH_i \in \{VH\}$; NMZ — no protection mechanism to ensure the i -th counter threats.

If all $i = m$, $a_{mj}^{DFSZ} = NMZ$, Then concludes that TZZI ABS can not protect BIn from this destructive influence and thus to increase the level of security of ABS must raise additional funds for protection mechanisms.

Step 3.2 Defining the requirements of regulators $\{RR^{ABS}\}$ That includes requirements for security BIn — $\{R_{BBI}\}$, defined in international and national standards set degree assessments meet the requirements of safety $\{OV_{BBI}\}$ and set the final level of compliance with the safety requirements set BIn $\{IU_{BBI}\}$:

$$\{RR^{ABS}\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}. \quad (5.41)$$

Suppose that this figure is performed.

Step 3.3 Definition of generalized index of security of ABS, which allows you to assess the level of compliance and regulatory requirements TZZI determined:

$$OPZ^{ABS} = \sum_{i=1}^k OPZ_i, \quad (5.42)$$

where: k — number of individual safety parameters; OPZ_i — okremy index takes the value from the set: OPZ_1 — no unacceptable risks, if in OPS threats in the preparation of model/models offender and found unacceptable risk to the level of risk is $OPZ_1 = 0$, otherwise — $OPZ_1 = 1$; OPZ_2 — no dangerous threats closure mechanisms TZZI, $OPZ_2 = 0$, if the OPS in the preparation of a model found “unbalanced” threat — $OPZ_2 = 1$; OPZ_3 — level security compliance requirements BIn regulators recommended recognized — $OPZ_3 = 1$, if deemed unauthorized — $OPZ_3 = 0$.

Based on the generalized index of protection OPZ^{ABS} , generalized synergetic threat $W_{synerg}^{IB,KB,BI}$, a plurality of assets BIn $I_{A_i} = (Type, A^C, A^D, A^A, A^K, C_Y)$

and the proposed model for evaluating investments in IS BIn in ABS (see pidrozd. 4.1) is determined by the state of the model of efficiency investments in IB BIn OPS. Initial data for evaluation are the main figures on the basis of the consolidated financial statements under International Financial Reporting Standards and Independent Auditor’s Report Bank “Privat Group” in 2015, 2016 (https://bank.gov.ua/control/uk/publish/article?art_id=34661442). That are listed in the table 5.12. In the calculations take into account that for IB in ABS bank spent 4 % of annual income, development costs TTZI up to 2 % of annual profits NPV_{zbszi}^{ABS} —

the likely cost of removal without compromising security applied to 25 % of annual profits NPV_{zbtshi}^{ABS} — the likely cost of eliminating compromising safety to 2 % of annual profits S_{sz} — cost means of protecting 30 % of the total value of information assets BIn. The discount rate is 13 % (http://bank-ua.com/%D0%9E%D0%B1%D0%BB%D1%96%D0%BA%D0%BE%D0%B2%D0%B0_%D1%81%D1%82%D0%B0%D0%B2%D0%BA%D0%B0_%D0%9D%D0%91%D0%A3).

Table 5.12. — Output data

Year	C_{prib}^{ABC}	I_{inv}^{ABC}	N (Period)	r (%)
2015	7261000000	145220000	2	13
2016	2448000000	48960000	2	13

Estimated investment in IB BIn in ABS is determined by the following steps:

Step 1. Evaluation of return on investment in information security:

$$ROI^{ABS} = NPV_{inv}^{ABS} - NPV_{zt}^{ABS}, \quad (5.43)$$

where: NPV_{inv}^{ABS} — Income from investments in TZZI ABS;

NPV_{zt}^{ABS} — expenses in TZZI ABS;

ROI^{ABS} — profitability of TZZI investments in ABS.

The calculation results are presented in Table 5.13.

Table 5.13. — Background information on the assets in the BIn ABS (thousand USD)

Name, I_{A_i} % of C_{prib}^{ABC}	u_j	NPV_{inv}^{ABS}	NPV_{zt}^{ABS}	ROI^{ABS}	S_{sz}
BT (20 %)	24 480 000	24 480 000	7 344 000	17 136 000	7 344 000
PID (5 %)	6 120 000	6 120 000	1 836 000	4 284 000	1 836 000
CrD (30 %)	36 720 000	36 720 000	11 016 000	25 704 000	11 016 000
KT (20 %)	24 480 000	24 480 000	734 000	17 136 000	734 000
StO (3 %)	3 672 000	3 672 000	1 101 600	2 570 400	1 101 600
Ol (2 %)	2 448 000	2 448 000	734 400	1 713 600	734 400
YI (10 %)	12 240 000	12 240 000	3 672 000	8 568 000	3 672 000
PD (10 %)	12 240 000	12 240 000	3 672 000	8 568 000	3 672 000

Step 2. Measuring return on investment in TZZI:

$$ROSI^{ABS} = NPV_{zbtshi}^{ABS} - NPV_{zvtshi}^{ABS}, \quad (5.44)$$

where: NPV_{zbtshi}^{ABS} — the cost of eliminating compromising security without the use of means of protection (TZZI);

NPV_{zvtshi}^{ABS} — the cost of eliminating compromising safety using TZZI.

The calculation results are presented in Table 5.14.

Table 5.14. — Evaluation results ROI (thousand USD)

Name, I_{A_i}	$NPV_{zbt\text{sz}i}^{ABS}$	S_{sz}	ALE_i	NPV_{zvtszi}^{ABS}	$ROSI^{ABS}$
BT	122 400 000	7 344 000	16 279 200	34 272 000	88 128 000
PID	30 600 000	1 836 000	4 069 800	8 568 000	22 032 000
KrD	183 600 000	11 016 000	24 418 800	51 408 000	132 192 000
KT	122 400 000	734 000	16 279 200	34 272 000	88 128 000
StO	18 360 000	1 101 600	1 733 184	5 140 800	13 219 200
Ol	12 240 000	7 344 000	682 992	3 427 200	8 812 800
YI	61 200 000	3 672 000	5 777 280	17 136 000	44 064 000
PD	61 200 000	3 672 000	8 139 600	17 136 000	44 064 000

Step 3. Evaluation of net present value:

$$NPV_{zvtszi}^{ABS} = C_{sz} + \sum_{i=1}^N \frac{ALE_i}{(1+r)^i}, \quad (5.45)$$

where: N — number of intervals investments;

ALE_i — expected to cost i -th period;

r — discount rate;

C_{sz} — cost remedies.

The results are shown in Table 5.14.

Step 4. BIn risk assessment methodology of calculation Annual loss expectancy — ALE , is the expected loss in each period of evaluation:

$$ALE^{ABS} = \sum_{i=1}^n I(O_{DF}^{ABS}) F_i, \quad (5.47)$$

where: $\{O_{DF}^{ABS}\}$ — set of threats;

$I(O_{DF}^{ABS})$ — cost implications of the threat;

ALE^{ABS} — the expected damage from the sale of threats;

F_i — Frequency (feature) of threats.

The results are shown in Table 5.15.

Step 5. Evaluation of potential losses U^{ABS} information assets based expression (5.30) and Table 5.9:

$$U^{ABS} = p_{rj} u_j, \quad (5.45)$$

where: p_{rj} — probability of realization of at least one threat j -th asset;

u_j — j -th value of the asset.

The results are shown in Table 5.15.

Table 5.15. — The evaluation of potential losses U^{ABS} .
Determining the probability of at least one threat to each asset Bln

<i>ID of threats</i>	<i>BT</i>	<i>PID</i>	<i>CrD</i>	<i>KT</i>	<i>StO</i>	<i>Ol</i>	<i>YI</i>	<i>PD</i>
02.03.01.05	131212.8	32803.2	196819	131213	17699	7,490.88	58997	65606
03.03.03.04	162547.2	40636.8	243821	162547	12191	3,231.36	40637	81274
03.03.02.03	162547.2	243821	162547	18286.6	8,127.36	8,127.36	60955	81274
03.03.02.05	163036.8	40759.2	244555	163037	16377.1	5,532.48	54590	81518
03.02.04.03	162547.2	40636.8	243821	162547	16303.7	9,253.44	54346	81274
02.02.04.05	131212.8	131213	196819	131213	13219.2	2,252.16	44064	65606
02.02.02.03	97920	97920	146880	97920	4896	2448	24480	48960
01.02.03.02	131212.8	131213	32803.2	196819	9,840.96	5,238.72	32803	65606
03.02.03.01	130723.2	32680.8	196085	130723	16891.2	9,938.88	56304	65362
03.02.02.03	131212.8	32803.2	196819	131213	17699	10869.12	58997	65606
...	...	...	...	...	...	...	...	...
03.03.02.03	130723.2	32680.8	196085	130723	14688	5,483.52	48960	65362
01.01.03.05	65116.8	16279.2	97675.2	65116.8	8,372.16	4,944.96	27907	32558
03.03.02.04	162547.2	40636.8	243821	162547	14614.6	5,679.36	48715	81274
03.01.03.02	130723.2	32680.8	196085	130723	13366.1	4,602.24	44554	65362
01.01.03.04	162547.2	40636.8	243821	162547	21958.6	9,253.44	73195	81274
3.01.01.01	97920	24480	146880	97920	13659.8	4,210.56	45533	48960
03.01.04.01	64627.2	16156.8	96940.8	64627.2	9,694.08	3,231.36	32314	32314
03.01.04.05	131212.8	32803.2	196819	131213	18286.6	5630.4	60955	65606
03.01.04.05	131212.8	32803.2	196819	131213	19681.9	4,602.24	55814	65606

Step 6. Evaluation of total expected loss:

$$OU^{ABS} = \sum_{j=1}^n U^{ABS}. \quad (5.48)$$

The results are shown in Table 5.15.

Step 7. Evaluation of the total cost of spending eliminate the consequences of threats and other causes disabling TZZI:

$$M^{ABS} = \sum_{i=1}^m C_i, \quad (5.49)$$

where: C_i — the value of i -th event;

m — the total number of steps taken.

The results are shown in Table 5.16.

Table 5.16. — Results of total expected loss effects of disabling TZZI Thousand. USD.

Name I_{A_i}	OU^{ABS}	M^{ABS}	Fishburne weights				W_{ABS}^{effinv} components for security services			
			w_{FC}	w_{HL}	w_{IA}	w_{IAu}	WITH	AND	AND	Au
BT	16 279 200	122 400 000	0.4	0.3	0.2	0.1	48 960 000	36 720 000	244 800 000	12 240 000
PID	4 069 800	30 600 000	0.4	0.3	0.2	0.1	12 240 000	9 180 000	55 080 000	36 720 000
CrD	24 418 800	183 600 000	0.4	0.3	0.2	0.1	73 440 000	55 080 000	36 720 000	183 600 000
KT	16 279 200	122 400 000	0.4	0.3	0.2	0.1	48 960 000	36 720 000	244 800 000	12 240 000
StO	1 733 184	18 360 000	0.4	0.3	0.2	0.1	7 344 000	5 508 000	36 720 000	18 360 000
Ol	682 992	12 240 000	0.4	0.3	0.2	0.1	4 896 000	3 672 000	24 480 000	1 224 000
YI	5 777 280	61 200 000	0.4	0.3	0.2	0.1	24 480 000	18 360 000	12 240 000	612 000
PD	8 139 600	61 200 000	0.4	0.3	0.2	0.1	24 480 000	18 360 000	12 240 000	612 000

Step 8. Definition of integral criterion of efficiency investments in the security BIn OPS:

$$W_{ABS}^{effinv} = \sum_{i=1}^N w_i M^{ABS}, \quad (5.50)$$

where $w_i \in [0;1]$, $W_F^{ABS} = \sum_{i=1}^N w_i$ — the system of Fishburne weighting coefficients, $i \in [1;N]$.

Each parameter is assigned weight classes Fishburne rule [65], based on the fact that change is subject to criteria weighting coefficients descending arithmetic progression.

In this first criterion ($i=1$), is the first in a strictly ordered by importance criteria ranked number $i=1, 2, \dots, n$, is the most important and has the greatest weight. This rule is given by the expression:

$$w_i = \frac{2(N-n+1)}{N(N+1)}, \quad (5.51)$$

where: w_i — weight Fishburne;

N — total number of parameters;

n — serial number parameter;

i — number of parameters.

According to the Fishburne expression:

$$w_1 = \frac{2 \times N}{N(N+1)}, \quad w_N = \frac{2}{N(N+1)}, \quad \gamma = \frac{w_1}{w_N} = N, \quad (5.52)$$

where γ — the multiplicity of weighting coefficients differences from each other.

So, $w_i^C = 0.4$, $w_i^I = 0.3$, $w_i^A = 0.2$, $w_i^{Au} = 0.1$.

For the valuation obtained values of W_{ABS}^{effinv} divide the results by 108 and use the approach of forming a common index $W_{synerg}^{IB,KB,BI}$.

Results are shown in Table 5.17.

$$W_{ABS_{genl_{A_i}}}^{effinv C} = \sum_{i=1}^{A_i} W_{ABS}^{effinv C} \text{ — the total figure for the service, confidentiality,}$$

$$W_{ABS_{genl_{A_i}}}^{effinv I} = \sum_{i=1}^{A_i} W_{ABS}^{effinv I} \text{ — the total figure for the service integrity,}$$

$$W_{ABS_{genl_{A_i}}}^{effinv A} = \sum_{i=1}^{A_i} W_{ABS}^{effinv A} \text{ — the total figure for service availability,}$$

$$W_{ABS_{genl_{A_i}}}^{effinv Au} = \sum_{i=1}^{A_i} W_{ABS}^{effinv Au} \text{ — the total figure for the service authenticity.}$$

The overall indicator is defined by the expression:

$$W_{ABS_{gen}}^{effinv} = W_{ABS_{genI_{A_i}}}^{effinv} \cap W_{ABS_{genI_{A_i}}}^{effinv} \cap W_{ABS_{genI_{A_i}}}^{effinv} \cap W_{ABS_{genI_{A_i}}}^{effinv}. \quad (5.51)$$

Table 5.17. — Results overall performance indicator

Name, I_{A_i}	W_{ABS}^{effinv} components for security services			
	$WITH$	AND	AND	Au
BT	0.04896	0.03672	0.02448	0.01224
PID	0.01224	0.00918	0.05508	0.00367
CrD	0.07344	0.05508	0.03672	0.01836
KT	0.04896	0.03672	0.02448	0.01224
StO	0.007344	0.005508	0.003672	0.001836
Ol	0.04896	0.03672	0.02448	0.01224
YI	0.02448	0.01836	0.01224	0.00612
PD	0.02448	0.01836	0.01224	0.00612
$W_{ABS_{genI_{A_i}}}^{effinv}$	0.2448	0.1836	0.1224	0.0612
$W_{ABS_{gen}}^{effinv} = W_{ABS_{genI_{A_i}}}^{effinv} \cap W_{ABS_{genI_{A_i}}}^{effinv} \cap W_{ABS_{genI_{A_i}}}^{effinv} \cap W_{ABS_{genI_{A_i}}}^{effinv} \cap W_{ABS_{genI_{A_i}}}^{effinv} = 0.00034$				

To evaluate the quality of service facilities for the safety of ABS BI will use the proposed methodology for assessing functional efficiency of data exchange network ABS, which is based on a simple multivariate analysis, which takes into account both technical data networks (data rate, probability and package delivery time, etc.), safety technical information security, and economic parameters (price scale, service network, the efficiency of investment in safety, etc.).

The method comprises four steps:

- 1) definition of sustainability cryptographic method of rapid analysis based on entropy method for assessing the initial random order.
- 2) determine the impact of security threats to the components, IB, CB, BI based on their synergy and hybridity.
- 3) definition of investment in the security BI in ABS.
- 4) determine the effectiveness of the ABS data exchange through an integrated indicator.

Stage 1. *Determination of cryptographic method of rapid analysis based on entropy evaluation method chance original sequence* (see subsections 4.2, 5.1). The result of research is to assess the maximum table encryption BIn (table 5.18).

Table 5.18. — Estimated maximum cryptographic protection

№	Code	Entropy Open. Text (H_M)	Entropy crypto- grams (H_C)	Difference $H_{Cypher} =$ $= H_C - H_M$	Chance of en- cryption, P_C
1.	Cellular automa- ta rule “60”	0.5023775 (5.023775)	0.6820179 (6.820179)	0.1796404 (1.796404)	0.637079949
2.	Secure Random Generator PVP	0.5023767 (5.023767)	0.7999982 (7.999982)	0.2976215 (2.976215)	0.747287753
3.	DES	0.469276	0.812043	0.342767	0.812043
4.	3DES	0.469276	0.812043	0.342767	0.812043
5.	GOST 28147–89	0.469276	0.811348	0.342072	0.811348
6.	Kalina-256	0.469276	0.954519	0.485243	0.954519
7.	AES-256	0.469276	0.95454	0.485264	0.95454
8.	RSA	0.469276	1.000	0.530724	1.000
9.	HCCDUC from MEC (HCCDC)	0.469276	0.98764	0.518364	0.98764
10.	Ideal cipher		1.000		1.000

Stage 2. *Determining the impact of security threats to the components, IB, CB, BI based on their synergy and hybridity.*

Based on classifier, taking into account the expressions (5.8)–(5.12) is determined generalized synergetic probability of realization attack on BIn in ABS — $W_{synerg}^{IB,KB,BI}$.

The stability of security in ABS on the possible actions of the attacker based on the theorem of multiplication probabilities of independent events:

$$B = P_A \times W_{synerg}^{IB,KB,BI}, \quad (5.54)$$

where: B — the stability of the security in the ABS;

P_C — likelihood encryption TZZI in ABS.

Stage 3. *Definition of investment in the security BIn in ABS.*

Based on the expressions (5.22)–(5.29) and the proposed method is defined by a generalized indicator of the effectiveness of investment in IB BIn in ABS — W_{effinv} .

Stage 4. *Determination of the effectiveness of the ABS data exchange through an integrated indicator.*

Evaluating the effectiveness of data exchange is based on a comprehensive measure by the expression:

$$W(u_i) = \frac{n^{(u_i)} - t^{(u_i)}}{n^{(u_i)}} \times B^{(u_i)} \times P_{prp}^{(u_i)} \times W_{effinv} \times W_{norm}, \quad (5.55)$$

where: $W(u_i)$ — Network performance indicator at the chosen strategy (method of increasing probability) u_i ;

$n^{(ui)}$ — the number of information bits in the package chosen strategy u_i ;

$t^{(ui)}$ — the delivery package during t chosen strategy u_i ;

$B^{(ui)}$ — stability of security in ABS;

$P_{prp}^{(ui)}$ — reliability correct packet delivery at the chosen strategy;

U — set of admissible strategies (methods increase the probability used in the network);

$W_{eff}^{(ui)}$ — multi-rate efficiency, designed the proposed method;

W_{norm} — normalized multi-rate performance.

Initial data network ABS are the results table 5.19 based on reference table the parameters of the data taken into account in the integral index of the functional efficiency of the IP network ABS W_{norm} (see subsection 4.2).

Table 5.19. — Generalized efficacy data networks

Technology	Cost	Speed	The probability of packet delivery	delivery Time	delay package	Productivity	Consolidated Performance Index	The relative efficiency, %
Frame Relay	3	2	1	5	3	3	270	7.37
Fast Ethernet	3	2	2	4	3	3	432	11.79
10 Gb Ethernet	2	4	4	4	3	3	1152	31.45
40 Gb Ethernet	1	5	4	4	3	3	720	19.66
Total:							3663	100

Fig. 5.18 shows the results of research on the efficiency of service quality ABS facilities to ensure the security BIn.

Initial data for the study are: technology Frame Relay, 100 Mbit Ethernet, 10 Gbit Ethernet, 40 Gbit Ethernet with critical feedback and ARQ “Back-to-N”, $W_{synerg}^{IB,KB,BI} = 0.0022839$, $Gost - t_{sh} = t_{rozsh} = 0.033$ s, $RSA - t_{sh} = t_{rozsh} = 0.2$ s, HCCDUC with MEA — $t_{sh} = t_{rozsh} = 0.0015$ s, $P_C^{Gost} = 0.95454$, $P_C^{HCCDC} = 0.98764$, $P_C^{RSA} = 1.0000$, $n = 1518$, $C = 36\,000$, $P_{prp} = 0.9999$, $s = 32$, $w = 300\,000\,000$.

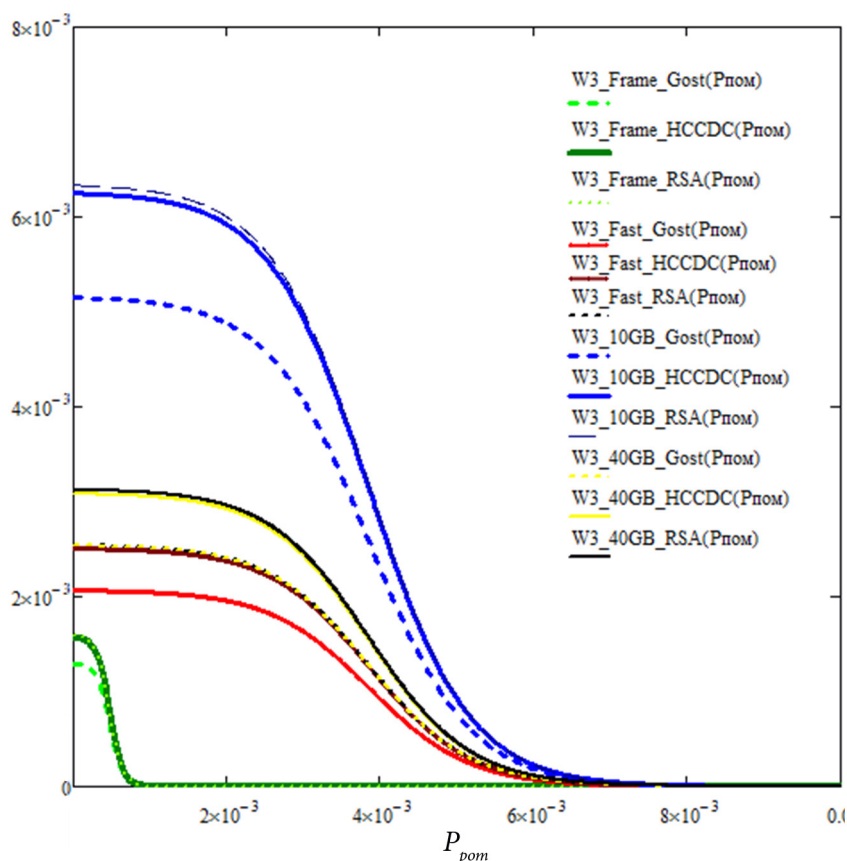


Fig. 5.18. The research results of the functional efficiency of the ABS ARQ "Back-to-N" using methods of evaluating investments in IS BIn in ABS

Analysis of Fig. 5.18 shows that the proposed method of estimating the functional efficiency without ABS allows significant time and cost of expert to assess the state of the ABS for users to use evaluation results for its scale, improving the technical performance of ABS, level IS BIn in ABS.

Thus, all formulated and applied scientific findings confirmed the results of the experiment.

5.4 Conclusions of the fifth section

The final section of the thesis the methodology of the system of IS BIn in ABS, which makes it possible to provide increasing levels IS BIn in ABS in terms of hybrid threats on the organization of the banking sector, the rational organization of the system for IB BIn in ABS in terms of simultaneous action

on the system of threats to information security kiberbezpetsi and safety information. As a result, the following results:

1. The verification and investigation of the adequacy of the proposed method of evaluating investments in IS BIn in ABS, methods of evaluation of the functional efficiency of the ABS data subject to the conditions of counteraction to threats hybrid IS, SC, SI on BIn in ABS.

2. The methodology of constructing a system of banking information security in automated banking systems, which unlike known approaches implements a radically new concept hybrid countering threats to the banking sector of the state. Its essence and meaning is the rational organization of information security software BIn in ABS in terms of simultaneous action on the system of information security threats, kiberbezpetsi and safety information. This approach allows to obtain full and adequate assessment of IS BIn in ABS, which significantly affect the value of investments in the safety of the banking sector and opens the way to make informed management decisions on security.

Thus, the proposed methodology allows for improving the safety BIn, to get the maximum number of emergent properties in terms of combating hybrid threats IS, CS, SI, namely: assessment of synergies and hybridity threats component safety: IS, CS, SI on BIn in ABS, minimization costs of investing in IB BIn, providing high speed crypto-conversion obrazovaniya and demonstrable level of stability in the integrated mechanisms to ensure the integrity, confidentiality, authenticity and reliability BIn in ABS with u I open channels of communication, functional assessment transmission efficiency BIn in ABS.

References in Chapter 5

1. S. P. Evseev, D. V. Sumtsov, O. G. Korol', B. P. Tomashevskij Analiz jeffektivnosti peredachi dannyh v komp'juternyh sistemah s ispol'zovaniem integrirovannyh mehanizmov obespechenija nadezhnosti i bezopasnosti//Vostochno-evropejskij zhurnal peredovyh tehnologij, № 2/2(44), p. 45–49, 2010.
2. O. G. Korol' Otsinka jakosti obslugovuvannja global'noi merezhi na osnovi tehnologij Ethernet za dopomogoju kompleksnogo pokaznika//Sistemi obrobki informacii, № 2(148), p. 88–94, 2017.
3. S. P. Evseev, S. E. Ostapov, H. N. Rzaev, V. I. Nikolaenko Ocinka obminu danimi v global'nih obchisljuval'nih merezhah na osnovi kompleksnogo pokaznika jakosti obslugovuvannja merezhi//Naukovij zhurnal Radioelektronika, informatika, upravlinnja, № 1(40), p. 115–128, 2017.
4. O. O. Kuznetsov, S. P. Evseev, S. V. Kavun, O. G. Korol' Signali i kodi. Algebraichni metodi sintezu. Monografija. – Harkiv, Ukraine: HNEU, 2009.
5. R. Blejhut Theory and practice of error control codes. Translated from English. – M.: Mir, 1986.
6. J. Clark. Ml., J. Kane The coding error correction in digital communication systems. Translated from English. – M.: Radio and Communications, 1987.
7. F. J. MacWilliams, N. J. A. Sloane The Theory of Error-Correcting Codes. – M.: Svjaz', 1979.
8. V. M. Muter Osnovy pomehoustojchivoj teleperedachi informacii. – L.: Jenergoatomizdat. Leningr., 1990.
9. T. Kasami, N. Tokura, E. Iwadari, Ja. Inagaki Teorija kodirovanija. Translated from Japanese, B. S. Cybakova and S. I. Gel'fanda. – M.: Mir, 1978.
10. R. Grishhuk, O. Korchenko Metodologija sinteza i analiza differencial'no-igrovyh modelej i metodov modelirovanija processov kiberatak na gosudarstvennye informacionnye resursy//Nauchno-prakticheskij zhurnal "Zashchita informatsii", № 3, p.115–122, 2012.
11. G. Baranov, M. Zaharova, D. Gornickij Metodologija sinteza sistem ocenki urovnja zashhishhennosti gosudarstvennyh informacionnyh resursov ot sociotekhnicheskikh atak//Nauchno-prakticheskij zhurnal "Zashchita informatsii", № 3, p. 98–103, 2012.
12. O. Korchenko, M. Luckij, M. Zaharova, Ju. Drejs Metodologija sinteza i programmajaja realizacija sistemy ocenki ushherba nacional'noj bezopasnosti v sfere ohrany gosudarstvennoj tajny//Zashchita informatsii, vol. 15, № 1, p. 14–20, 2013.
13. S. Rajba, M. Karpinski, and O. Korchenko Generalized models, construction methodology and the application of secure wireless sensor networks

- with random network parameters//Informatsionnaya bezopasnost', № 2(20), p. 120–125, 2014.
14. O. Judin, S. Buchik Metodologija zashchity gosudarstvennykh informatsionnykh resursov. sravnitel'nyj analiz osnovnykh terminov i opredelenij// Nauchno-prakticheskij zhurnal "Zashchita informatsii", vol. 17, № 3, p. 218–225, 2015.
 15. B. Zhurilenko Metodologija postroenija i analiza sostojanija kompleksa tehniceskoy zashchity informacii s verojatnostnoj nadezhnost'ju i uchetom vremennykh popytok vzloma//Nauchno-prakticheskij zhurnal "Zashchita informatsii", vol. 17, № 3, p. 196–204, 2015.
 16. S. Buchik Metodologija analiza riskov dereva identifikatorov gosudarstvennykh informatsionnykh resursov//Nauchno-prakticheskij zhurnal "Zashchita informatsii", vol. 18, № 1, p. 81–89, 2016.
 17. A. Korchenko, V. Shherbina, N. Vishnevskaja Metodologija postroenija sistem vyjavlenija anomlij porozhdennykh kiberatakami//Zashchita informatsii, vol. 18, № 1, p. 30–38, 2016.
 18. E. Ivanchenko, S. Kazmirchuk, A. Gololobov Metodologiya sinteza sistem analiza i otsenki riskov poter' informatsionnykh resursov//Zashchita informatsii, vol. 14, № 2, p. 24–28, 2012.
 19. A. Shiyan Metodologiya kompleksnoy zashchity cheloveka i sotsial'nykh grupp ot negativnogo informatsionno-psikhologicheskogo vozdeystviya// Informatsionnaya bezopasnost', № 1(22), p. 94–98, 2016.
 20. A. Korchenko, S. Kazmirchuk, E. Ivanchenko Metodologiya sinteza adaptivnykh sistem otsenivaniya riskov bezopasnosti resursov informatsionnykh sistem//Zashchita informatsii, vol. 19, № 3, p. 198–204, 2017.
 21. The doctrine of information security of Ukraine, approved by the Decree of the President of Ukraine dated February 25, 2017, No. 47/2017. URL: <http://zakon3.rada.gov.ua/laws/show/47/2017/paran2#n2>.
 22. Ukaz Prezidenta Ukrainy ot 15 marta 2016 № 96 "O reshenii Soveta natsional'noy bezopasnosti i oborony Ukrainy ot 27 yanvarya 2016 goda. O Strategii kiberbezopasnosti Ukrainy". URL: <http://zakon3.rada.gov.ua/laws/show/96/2016/paran11#n11>.
 23. Decree of the President of Ukraine dated February 12, 2007 No. 105 "On the Strategy of National Security of Ukraine". URL: <http://zakon3.rada.gov.ua/laws/show/105/2007>.
 24. R. V. Grishchuk, Yu. G. Danik Sinergiya informatsionnykh i kiberneticheskikh deystviy//Proceedings of the NUOU, № 6(127), p. 132–143, 2014.
 25. V. L. Buryachok, R. V. Grishchuk, V. A. Khoroshko Politika informatsionnoy bezopasnosti/edited by prof. V. A. Khoroshko. – K.: ChPP «Zadruga», 2014.

26. Yu. G. Danik et al. Osnovy zashchity informatsii. Tutorial. – Zhitomir: ZhVI DUT, 2015.
27. A. K. Yudin Informatsionnaya bezopasnost'. Normativno-pravovoe obespechenie. – M.: NAU, 2011.
28. R. V. Grishchuk, Yu. G. Danik Osnovy kiberbezopasnosti/ed. by prof. Yu. G. Danika. – Zhitomir: ZHNAEU, 2016.
29. I. S. Ivanchenko, V. A. Khoroshko, Yu. E. Khokhlachova, D. V. Chirkov Obespechenie informatsionnoy bezopasnosti gosudarstva/edited by prof. V. A. Khoroshko. – K.: ChPP “Zadruga” 2013.
30. A. G. Korchenko, A. E. Arkhipov, Yu. A. Dreys Otsenivanie vreda natsional'noy bezopasnosti Ukrainy v sluchae utechki gosudarstvennoy tayny. Monografiya. – K.: NA SBU Ukrainy, 2014.
31. A. A. Korchenko, L. N. Skachek, V. A. Khoroshko Bankovskaya bezopasnost. Uchebnik/edited by prof. V. A. Khoroshko. – K: ChPP “Zadruga”, 2014.
32. V. I. Yarochkin Bezopasnost' bankovskikh sistem. – M.: Publisher: Os'-89, 416 p., 2012.
33. A. Potiy, D. Pilipenko Kontseptsiya strategicheskogo upravleniya informatsionnoy bezopasnost'yu//Radioelektronnye i komp'yuternye sistemy, № 6(47), p. 53–58, 2010.
34. M. Barilyuk Metodicheskiy podkhod k formirovaniyu organizatsionno-ekonomicheskogo obespecheniya upravleniya finansovoy bezopasnost'yu kommercheskogo banka//Biznesinform, № 6, p. 191–200, 2017.
35. S. Evseev Analiz zashchity v natsional'noy sisteme masovykh elektronnykh platezhey//Informatsionnaya bezopasnost', № 3(15), № 4(16), p. 15–28, 2014.
36. S. Evseev, O. Korol', G. Kots Analiz zakonodatel'noy bazy k sisteme upravleniya informatsionnoy bezopasnost'yu NSMEP//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, ed. 5/3(77), p. 48–59, 2015.
37. S. Evseev Metodologiya otsenivaniya bezopasnosti informatsionnykh tekhnologiy avtomatizirovannykh bankovskikh sistem Ukrainy//Nauchno-tekhnicheskii zhurnal “Zashchita informatsii”, vol. 22, № 2, p. 297–309, 2016.
38. Briones, P. Chamoso, A. Barriuso Review of the Main Security Problems with Multi-Agent Systems used in E-commerce Applications”//ADCAIJ, Regular Issue, Vol. 5, N. 3, p. 55–61, 2016.
39. W. Simpson Securing Information Systems in an Uncertain World Enterprise Level Security//Systemics, Cybernetics and Informatics, Vol. 14, № 2, p. 83–90, 2016.
40. S. Evseev, O. Korol', A. Sochneva Analiz otsenki riskov kiberbezopasnosti bankovskoy informatsii//Sbornik nauchnykh trudov NAU “Zashchita informatsii”, ed. 23, p. 109–129, 2016.

41. R. Grishchuk, S. Evseev The synergetic approach for providing bank information security: the problem formulation//Informatsionnaya bezopasnost', № 22(1), p. 64–74, 2016.
42. S. Evseev Model' narushitelya prav dostupa v avtomatizirovannoy bankovskoy sisteme na osnove sinergeticheskogo podkhoda//Informatsionnaya bezopasnost', № 2(26), p. 110–120, 2017.
43. Yu. Maliy Metodicheskie podkhody k analizu ugroz bezopasnosti informatsii i riskov v bankovskoy sfere//Vestnik BUKER, № 1, p. 135–140, 2013.
44. S. Vasil'chenko Nekotorye aspekty metodologicheskoy osnovy modelirovaniya finansovoy bezopasnosti banka//Ekonomika, № 6(147), p. 15–19, 2013.
45. S. Evseev Sinergeticheskaya model' otsenki bezopasnosti bankovskoy informatsii//Informatsionnaya bezopasnost', № 4(24), p. 104–118, 2016.
46. S. Evseev Otsenka effektivnosti investitsiy v bezopasnost' organizatsiy bankovskogo sektora na osnove sinergeticheskoy modeli ugroz//Sistemy obrabotki informatsii, № 2(148), p. 88–94, 2017.
47. O. Markova Sovershenstvovanie informatsionnoy bezopasnosti elektronnykh raschetov v kommercheskikh bankakh Rossii//Finansovaya analitika: problemy i resheniya, № 31, p. 38–49, 2015.
48. S. Evseev, S. Ostapov, Kh. Rzaev, V. Nikolaenko Otsenka obmena dannymi v global'nykh vychislitel'nykh setyakh na osnove kompleksnogo pokazatelya kachestva obsluzhivaniya seti//Nauchnyy zhurnal Radioelektronika, informatika, upravlenie, № 1(40), p. 115–128, 2017.
49. S. Evseev, O. Korol', Kh. Rzaev, Z. Imanova Razrabotka modifitsirovannoy nesimmetrichnoy krypto-kodovoy sistemy Mak-Elisa na ukorochennykh ellipticheskikh kodakh//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, vol 4. 9(82), p. 18–26, 2016.
50. S. Evseev, Kh. Rzaev, A. Tsyganenko Analiz programmnoy realizatsii pryamogo i obratnogo preobrazovaniya po metodu nedvoichnogo ravnovesnogo kodirovaniya//Bezopasnost' informatsii, vol. 22, № 2, p. 196–203, 2016.
51. S. Evseev, O. Korol', G. Kots Construction of hybrid security systems based on the crypto-code structures and flawed codes//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, 4/9(88), p. 4–21, 2017.
52. S. Evseev Ispol'zovanie ushcherbnykh kodov v krypto-kodovykh sistemakh//Sistemy obrabotki informatsii, № 5(151), p. 109–121, 2017.
53. S. Evseev, A. Androshchuk, V. Fedorchenko Postroenie sistem bezopasnosti informatsionno-telekommunikatsionnykh sistem na osnove kompleksnogo krypto-graficheskogo podkhoda//Sbornik nauchnykh trudov Nats. akademii Gos. prikor. sluzhby Ukrainy im. Bogdana Khmel'nitskogo.

- Seriya: voennye i tekhnicheskie nauki/edited by Alekseenko B. M., № 2(72), p. 258–268, 2017.
54. C. Scheau, A. Arsene, G. Dinca Phishing and e-commerce: an information security management problem//Journal of Defence Resources Management, vol. 7, № 1(12), p. 129–140, 2016.
55. Ab. Alhothaily, A. Alrawais, T. Song, B. Lin, and X. Cheng QuickCash: Secure Transfer Payment Systems//Sensors, № 17, 1376, p. 1–20, 2017. doi:10.3390/s17061376.
56. O. Yusupova Bezopasnost' tranzaktsiy pri ispol'zovanii internet-bankinga//Finansovaya analitika: problemy i resheniya, № 35, p. 26–40, 2016.
57. S. Evseev, O. Korol' Issledovanie metodov dvukhfaktornoy autentifikatsii//Sistemy obrabotki informatsii, № 2(118), p. 81–87, 2014.
58. S. Evseev, V. Abdulaev Algoritm monitoringa metoda dvukhfaktornoy autentifikatsii na osnove sistemy Passwindow//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, ed. 2/2(74), p. 9–15, 2015.
59. S. Evseev, G. Kots, E. Lekarev Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, 6/4(84), p. 11–23, 2016.
60. S. Evseev, O. Korol', G. Kots, S. Minukhin, A. Kholodkova The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, 5/9(89), p. 19–36, 2017.
61. Bank dannykh ugroz bezopasnosti informatsii. URL: <http://bdu.fstec.ru/vul>. Accessed on: 5.12.2017.
62. S. Yevseiev, V. Ponomarenko, O. Rayevnyeva Evaluation of the functional efficiency of the corporate scientific-educational network based on complex quality of service indicators//Vostochno-evropeyskiy zhurnal peredovykh tekhnologiy, 6(90), 2017 (Scopus).
63. R. Grishchuk, S. Evseev Metodologiya postroeniya sistemy obespecheniya informatsionnoy bezopasnosti bankovskoy informatsii v avtomatizirovannykh bankovskikh sistemakh//Bezopasnost' informatsii, 2017.
64. V.M. Postnikov, S.B. Spiridonov Metody vybora vesovykh koeffitsientov lokal'nykh kriteriev. Izdatel' FGBOU VPO "MG TU im. N.E. Bauman". № FS 77–48211, Ed. № 3, p. 267–287, 2016.
65. Postanova NBU28.09.2017 № 95, "Ob utverzhdenii Polozheniya ob organizatsii meropriyatiy po obespecheniyu informatsionnoy bezopasnosti v bankovskoy sisteme Ukrainy". URL: <http://zakon2.rada.gov.ua/laws/show/en/v0095500–17/page>. Accessed on: 5.12.2017.

CONCLUSIONS

The result of the work done is to solve urgent and important scientific and applied problems of methodology of constructing a system of information security in automated banking systems to enhance the level of protection against security threats hybrid nature.

In carrying out the thesis, the following key results are:

1. Analysis of current models, methods and systems for information security in the banking information ABS OPS as part of the critical infrastructure cybernetic state. It is established that the vast majority of known studies focused on the development or general approaches to IB bin in ABS or create methods, models and tools provide model-based SIA, which does not fully take into account modern requirements and approaches to building a system for IB bin in ABS. Unresolved part of the overall problem with bin questions remain developing integrated scientific and reasonable methodology for constructing practical systems for IB bin in ABS, development and implementation of a comprehensive information security system (CISS) integrated mechanisms ISS with software requirements for performance and likelihood circulation bin in ABS. The results of the analysis made it possible to clearly define the objectives of the research to develop the methodology for constructing systems for IB bin in ABS.

2. The concept of building a synergetic model of threats IB bin in ABS, basis of which is a three-tier security model of strategic management of banking information technologies. The concept covers all main areas of the bank's activities to ensure information security, based on a synergetic approach to the selection of the most effective ways achieving goals IB bin in ABS to the value of risk at every level model of strategic management of the bank and provides effective control over the implementation of ISMS functions OPS.

3. A software tool that implements advanced classification of banking information security threats in automated banking systems, which in contrast to the known synergistic model based threats, which allowed to classify threats by security components, types of services and infrastructure hierarchy levels of automated banking systems. Practical implementation allows on-line form expert evaluation of threats, analyze synergies and hybridity, assess the likelihood of the impact of these threats to information security of banking information without significant cost investment and human resources (electronic access to the resource: <http://skl.hneu.edu.ua>).

4. Practical method for evaluation of information security in the banking information ABS synergetic model based threats generalized model of offender assessment model security bin in ABS and ABS models of infrastructure to

optimize the cost of funds for the construction of a system for IB bin in ABS. The practical significance is the ability to timely evaluation of the relationships between assets Bean, infrastructure elements ABS, ABS TIP and possible signs of threats IB, CB, IB, which allows time to adjust the guidelines of the Bank of IB, plan investment in TIP, generate preventive measures to prevention of threats.

5. Developed method to ensure the confidentiality and integrity bin in ABS on hybrid crypto-code designs on unprofitable codes. The method is based on a modified crypto-code system to McEliece modified geometric codes that are integrated (a mechanism) provides IB bin (safe time — $TB > 200$ g., Resistance to cryptanalysis $LCD < 10-25-10-35$ group operations), transmission reliability bin in ABS ($R_{pom} < 9.10$), and reduce energy costs in their practical implementation in 10–12 times (encryption, decryption) by decreasing order of $GF(q)$. Implementation of the proposed methods can improve security bin in ABS.

6. The method of two-factor authentication based on McEliece and Niederreiter of MEC that ensures stability OTP-level passwords during transmission channels of communication open and to keep the possibility of further use of two-factor authentication protocol based on SMS-messages. Despite the decrease in power Galois field to $GF(26)$ for MACCS and $GF(24)$ for HCCC statistical characteristics of crypto-code constructions were at least no worse than traditional NCN McEliece in $GF(210)$. All cryptosystem tests were 100 %, and showed the best result in shortened HCCC MEC: 155 189 tests completed at 0.99, which is 82 % of the total number of tests. This traditional NCN McEliece in $GF(210)$ 149 tests showed at 0.99.

7. A method for evaluating the effectiveness of investments in the banking information security in automated banking systems which is based on a composite index investing to optimize the cost of funds for the construction of a system of information security in terms of hybrid threats of information cybersecurity and safety information. The practical implementation of the method allow to assess key indicators of investment in IT security given bin synergistic evaluation of threats IB, CB, BI.

8. A method for evaluating the functional efficiency of data exchange network ABS, which is based on a simple multivariate analysis, which takes into account both technical data networks (data rate and the probability of the delivery package and so on), technical protection of information, as and economic parameters (price scale, service network, the efficiency of investment in safety, etc.). The proposed method of estimating the functional efficiency of ABS allows without significant time and cost to conduct expert evaluation of ABS for users to use the results of the evaluation of the functional efficiency

of ABS for its scale, improve technical performance network ABS information security of banking information.

9. The methodology of constructing a system of banking information security in automated banking systems, which unlike known approaches implements a radically new concept hybrid countering threats to the banking sector of the state. Its essence and meaning is the rational organization of information security software bin in ABS in terms of simultaneous action on the system of information security threats, cybersecurity and safety information. This approach allows to obtain full and adequate assessment of IB bin in ABS, which significantly affect the value of investments in the safety of the banking sector and opens the way to make informed management decisions on security.

Thus, the proposed methodology allows improving the safety bin, to get the maximum number of emergent properties in terms of combating hybrid threats IB, CB, BI, namely: assessment of synergies and hybridity threats component safety: IB, CB, BI on bin in ABS, minimization costs of investing in IB Bean, providing high speed cryptoconversion and level of stability in the integrated mechanisms to ensure the integrity, confidentiality, authenticity and reliability bin in ABS with open channels of communication, functional assessment transmission efficiency bin in ABS.

10. The developed algorithms and software, allowing to verify the proposed methods, models and methodologies and to confirm their effectiveness in the context of IB bin in ABS. The results of the thesis introduced the activity of LLC “Sayfer BIS” — implemented software library cryptographic information based on modified crypto code of Niederreiter — McEliece Elliptic public key codes from unprofitable codes. The software library cryptographic information used in the authentication subsystem internet banking “ELPay” (Act of 05/18/2017), “Microcrypt Technologies Ltd.” — designed library of cryptographic information used to program complex IM protection “Crypto-IM +” (act of implementation 30.11.2017) planned to use in the bank as a part of a prospective protocol 2FA together with LLC “TANTARIUM” (Act of 06/14/2017) and PAO “MEGABANK” (Act of 06/09/2017). The results of the thesis are used in the educational process Kharkiv S. Kuznets Kharkiv National University of Economic, Kharkiv National University “KPI” Fedkovych Chernivtsi National University to improve the efficiency of training specialists in information security.

Reviewers

Valeriy Dudykevych

Head of Western Regional Training and Research Center of Information Protection, Honored inventor of Ukraine, Doctor of Sciences, Professor, Head of Information Security Department

Lviv Polytechnic National University

Lviv, Kniaz 79005 Ukraine

+38 (032) 258-30-60 mob.: +38 (067) 730-70-57

E-mail: vdudykev @ gmail.com

Oleksandr Korchenko

Head of IT-Security Academic Department,
Professor, Dr Eng (Information Security),
Laureate of the State Prize of Ukraine in Science and Technology
IEEE Senior Member

National Aviation University

Kyiv, Kosmonavta Komarova ave.1, 03680 Ukraine

+38 (044) 406-79-42 mob.: +38 (066) 760-05-95

E-mail: icaocentre @ nau.edu.ua

Nadiia Kazakova

Head of Department of Automated systems and cybersecurity
Doctor of Technical Sciences, Associate Professor

Odessa State Academy of Technical Regulation and Quality

Kovalska str., 15, Odessa, Ukraine, 65020

E-mail: kaz2003@ukr.net

Ruslan HRYSHCHUK, Serhii YEVSEIEV, Alexander SHMATKO

**CONSTRUCTION METHODOLOGY OF INFORMATION
SECURITY SYSTEM OF BANKING INFORMATION
IN AUTOMATED BANKING SYSTEMS**

Monograph

Subscribe to print 25/12/2018. Format 60×90¹/₁₆.

Convent. printed sheets 17,85.

Offset Paper. Garinitura Minion Pro. Conv. Pec. liter. 11.

Edition of 500 copies.

Typeset in Berling by Ziegler Buchdruckerei, Linz, Austria.

Printed by Premier Publishing s.r.o. Vienna,

Vienna, Austria on acid-free paper.

Am Gestade 1, 1010 Vienna, Austria

pub@ppublishing.org, ppublishing.org