© Hryshchuk R., Yevseiev S. The synergetic approach for providing bank information security: the problem formulation // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 1, p. 64-74.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ / INFORMATION SECURITY MANAGEMENT

THE SYNERGETIC APPROACH FOR PROVIDING BANK INFORMATION SECURITY: THE PROBLEM FORMULATION

Ruslan Hryshchuk[1], Sergii Yevseiev[2]

[1]Zhytomyr Military Institute n.a. S.P. Korolyov, Ukraine,
[2]Simon Kuznets Kharkiv National University of Economics, Ukraine

Ruslan HRYSHCHUK, Dr. Sc.

Date and place of birth: 1981, Pischanytsya, Ovrutskyi Rayon, Zhytomyrska Oblast, Ukraine.
Education: Zhytomyr Military Institute of Radioelectronics n.a. S.P. Korolyov, 2003.
Affiliation and functions: Head of Information & Cybersecurity Department at Scientific Centre of Zhytomyr Military Institute n.a. S.P. Korolyov since 2015.
Research interests: information & cybersecurity of the state.
Publications: over 197 scientific publications including monographs, textbooks, papers & patents.
E-mail: Dr.Hry@i.ua

Sergii YEVSEIEV, Ph.D.

Date and place of birth: 1969, Hartsizk, Donetsk region, Ukraine.
Education: Kharkov Military University, 2002.
Affiliation and functions: Associate Professor of Information Systems since 2007.
Research interests: information & cybersecurity of the banking systems.
Publications: over 180 scientific publications including monographs, textbooks, papers & patents.
E-mail: serhii.yevseiev@hneu.net

Abstract. *Continuously increasing number of threats to the security of bank information in automated banking systems (ABS) leads to a decrease in the quality of banking services provided by banks at the national and international level, regardless of their form of ownership. This situation is not least caused by the imperfection in used today mechanisms for providing bank information security. The technological complexity of new unknown threats identification, as well as the increasing sophistication in the methods of their implementation leads to the pressing need of radical revision of the existing approaches for providing security. Existing approaches are known mainly as oriented to the aggregation of forces and means of providing the security of bank information, which often leads to incomplete overlapping spectrum of threats and irrational use of resources allocated for the security. Thus, it becomes clear that the development of a fundamentally new approach to provide security of bank information is a prerequisite for the provision of high quality banking services, which this article is devoted. With this purpose, the article proposed the synergetic model of bank information security threats, which is first time since the system has allowed revealing the positions of the current state of the research problem. It is shown and proved that at the present stage of science and technology development, bank information security should be based on a fundamentally new approach, which is proposed to be called synergetic. Its implementation will provide a synergetic effect on the interaction of selected safety profiles and, consequently, demonstrate qualitatively new and previously unknown emergent properties of security system. As part of the proposed approach, the problem of increasing the level of bank information security is formalized in a general way and identified further ways of solving it. It is shown that the absence of such decisions in a bank information systems determines the relevance of the chosen for research theme and its scientific priority.*

Key words: *automated banking system, bank information, security of information, information security, cyber security, synergetic model of security threats, synergetic security index, emergence.*

Introduction

An important role in providing national security of Ukraine and especially in its economic side is assigned to the processes related with the protection of public market fundamentals that define the economic component of the competition. The development of modern, economically sustainable and stable state is closely related with the development of market relations and cost-competitive economy, in which the banking sector has a key, and, as a rule, a backbone role.

The revolutionary changes in the last decade occurred in the electronics industry, combining info-communication and computer networks into a unified information and cyberspace, creation of automated banking systems (ABS) have substantially expanded range of services in the banking sector. Thus, the range of threats for the national economy has significantly increased. The key and most potentially unsafe of which is the threat of breakdown or takeover of the remote control in the ABS control processes. The consequences in case of absence or imperfection of ABS security mechanisms can have a huge and irreversible character, leading to the collapse of the financial and banking system of Ukraine in particular, and the economic collapse in the country as a whole. Therefore, the decision of the whole complex of issues related with providing cyber security, information security and security of information in the ABS should be solved in complex and inseparably from one another, harmoniously completing and filling up each other, if necessary. Simple aggregation of forces and means to provide safety in the ABS in each individual case is unreasonable from both practical and scientific points of view. The absence of other alternative approaches encourages the urgent necessary to solve the current problem - improve the security of information in the Ukraine's ABS based of new unknown until today approaches.

Literature analysis and problem formulation

It is known that computer systems and telecommunications provide the reliability of a huge number of information systems for different purposes, including banking. Most of these systems contain confidential information with limited access. Thus, the solution of the problem of data processing automation resulted in generation of new problem – problem of security of information [1–30].

Since its introduction the banks has invariably caused criminal interest. This interest has been associated not only with storage of money in the credit organizations, but also with fact that banks have been focused on an important and often sensitive information about the financial and economic activities of many people, companies, organizations and even whole states. At the same time, regardless of means, mechanisms and techniques for providing security of bank information another actual problem, and the second on the general account, is the problem of information security of individuals, society and the state in which a person - bank employee or its client - the most vulnerable link [3–7].

Computerization of bank activities enabled to significantly increase bank employees' productivity, implement new technologies in financial products. Internet banking today becomes widespread among banks and customers, the use of Internet resources as an alternative means of customer PIN code transmission to the bank not only leads to a reduction transmission costs, but also helps to improve bank competitiveness, increase the flexibility of bank customers. The main barriers on the way of internet banking usage are cybercrimes questions, the lack of trust and legal support absence [6]. As an example, it should be noticed that 90% of all bank sphere crimes are cybercrimes based on use of automated bank information processing systems (ABIPS) [2]. Therefore, the bank system protection itself needs to use powerful authentication and control actions for both internal users and customers. It is well-known that the most reliable protection can provide means of two-factor authentication as either electronic keys (tokens), or one-time password generators [12]. Data security during storage process requires use of encryption means, which can operate at either data warehouse or separate system component level, such as database tables. Security of ATM's and payment terminals must be provided with the use of anti-virus protection means. At the same time, specificity of such devices requires the use of additional security tools, including the creation of "closed software and hardware environment" eliminating the installation of any third-party software and external devices connection [3]. Thus, **problem of cyber security** is a third integral component on the way of solving problems with providing security of bank information [11–14].

To ensure the adequacy of the bank information security system, regardless of which part of its problem linked with information security or cyber security, is possible to apply the principles of the Risk Management method [4]. This method under the right approach will enable define and classify just in time all threats and in and, according to the probability of negative consequences of their possible manifestations adequately organize the security of bank information system. But considering imperfection of the principles of the method of risk management in the bank sphere, he still requires the necessary operational development in the context of the raised above problems.

It is said in [7] that security of information including bank information can be achieved only through an integrated use of the entire arsenal of available protection means in all the structural elements of the production system and at all stages of the technological processing cycle. Ignoring system analysis methodology for bank information system establishment based on the complexity, and sometimes on the inability to objectively verify established system effectiveness due to imperfect regulatory and methodological information security, especially in the field of indicators and criteria [5], is also creates barriers to find a solution of indicated problems. For example, the international standard for operations with bank chip cards (EMV), introduced in 2005, defines the physical, electronic and informational interaction between the credit card and payment terminals for financial transactions on the basis of

ISO/IEC 7816 standard for contact cards, and ISO/IEC 14443 for contactless cards.

Thus, in result of study the literature, we can conclude that a fundamentally new effect in bank information security can be achieved only if all the above means, methods, measures and security technologies combined into a single coherent mechanism further named synergy.

The aims and objectives of research

The aims of the work are to state problem of providing bank information security, to form necessary and sufficient conditions for the creation of a fundamentally new methodological basis, aimed at achieving synergies in the field of public and private commercial banking security protection systems.

To achieve this objective the following specific tasks were formulated:

– a comprehensive critical analysis of nature and content "Bank Information" category at the current stage of science and technology development , relevance and substance of the legislative and regulatory framework in the field of the banking transactions protection in public and private ABS;

– refinement and complement of set of actual bank information security threats with from the triune position of providing information security, security of information and cybersecurity in bank sphere as a basis for creating new synergetic approach in the field of ABS information security;

– formalization of the security problem essence and content of bank information on the basis of proposed synergetic approach.

A comprehensive critical analysis of nature and content "Bank Information" category at the current stage of science and technology development, relevance and substance of the legislative and regulatory framework in the field of the banking transactions protection in public and private ABS

Consider the rapid science and technology development during the last 10 years as well as intensive use of the latest high-tech solutions in bank sector, the nature and content of "bank information" category has changed significantly. Today, as we know, the banki information is a major component of modern ABS. According to this, and on the base of [8, 31], it can be noticed that under the bank information in the broadest sense, means the set of information associated with the by-laws and the Guidelines of the institution, the legal form of banking institutions, the current view of the institution and its employees, types and forms of bank services, the quantity and composition of customers, transactions on customer accounts, the presence of correspondent relations and technical provision of the bank.

Taking into account embrace width of bank information category and in order to further correct use, it is proposed attribute classification of bank information (Fig. 1).

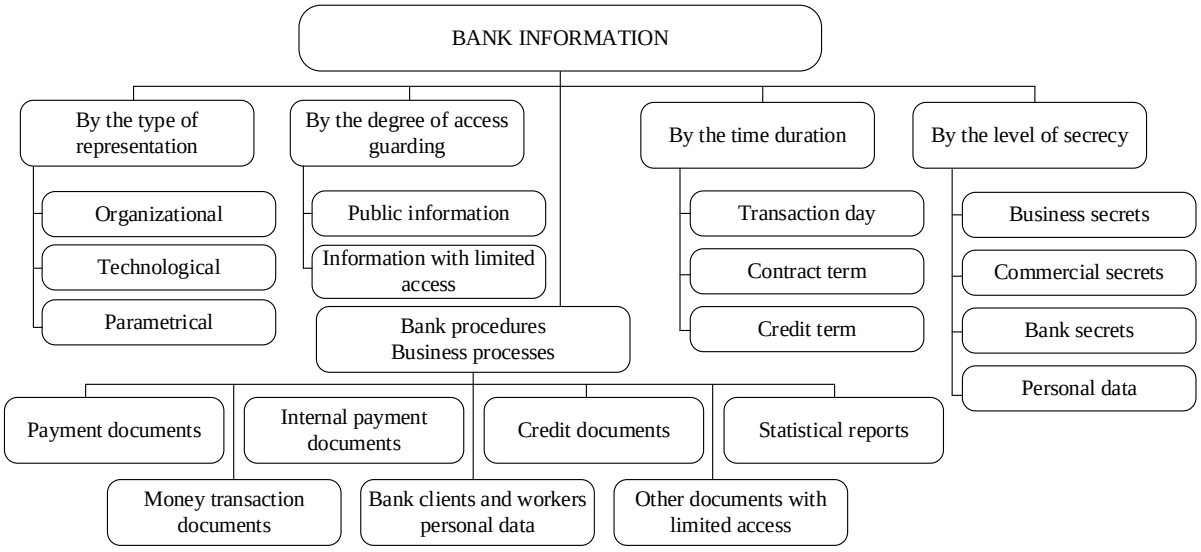

Fig. 1. Attribute classification of bank information

The advantage of the proposed attribute classification of bank information (see. Fig. 1) is that it in contrast to the known classification enables to reveal the depth of the content and essence of this category. For example, by types bank information splits on the organizational, technological and parametric. Organizational bank information means the information, which reflects character of business relations between bank and clients, information about organization features and the bank's management system construction. Technological bank information it is information about principles of bank's management while performing all bank activity types as well as information about usable high-end technological solutions in bank security systems. *Parametric bank information* is information, which reflects quantitative indicators, associated with bank capital and amount of its advances portfolio while performing all types of bank activity. Another advantage of the proposed classification is that in case of appearance of new attributes, which characterize different aspects of bank information category, the proposed classification provides possibility of expanding set of attributes.

From the proposed classification, it should be concluded that in the ABS subsystems circulated information of different confidentiality (secrecy) levels: from publicly available information, to information with limited access (commercial, banking and official secrecy). In the document ABS workflow are also presented: payment orders, other case and settlement documents, reports (financial, analytical, etc.), information about personal accounts, summary information and other confidential (restricted) documents, etc., which may also be referred to bank information.

Thus, in general, bank information is information which appears in result of bank activity. This is especially the information characterizing the bank itself, its financial situation, reliability and compliance with laws. Such information can be obtained from bank charter, its licenses, balance sheet, profit and loss statements and other sources. In addition, in a more narrow sense, bank information this is information about specific bank operations. Such information characterizes not only bank but also persons with whom bank enters into legal relations. As an example of bank information, it may be showed information about the availability of accounts or deposits, and operations with them, assets deposited at the bank.

Regardless of whether in a broad or narrow sense interpreted substantial part of the category of bank information activities of all the ABS subsystems in which it produced, processed, preserved and circulates is provided subject to the laws and recommendations of the National Bank of Ukraine. For this reason all the major existing regulations that regulate at the national level the above-described processes can be represented as a block diagram in a systematic form (Fig. 2).

The performed critical analysis of the Ukraine current regulatory environment has shown that in order to ensure the protection of information in ABS are used information security management systems (ISMS) for providing control of the functioning of complex information security systems. Thus, as the previous concluded, ABS is a comprehensive bank information system that integrates different areas of the bank's activities, the ability to automate and combine into unified whole financial institutions business processes. Complex system supporting centralized processing, multi-currency, and automation of key financial transactions should provide an effective management, control, receive reports about current activities of all of bank branches [9, 31].

Among the functions inherent in modern complex ABS, the following can be highlighted: transaction day; open-market operations, bank activities with security papers; intercompany activity; retail banking; online banking; e-banking; processing center and payment system (card products); bank back-office integration with its external transactions; bank operations management, business logic realization, control, tax accounting and reporting; risk management and strategic planning; customer loyalty programs, marketing, advertising and PR-services.

As known [2–7, 17, 18, 25–31], the main functions of ABS are implemented by using the following technologies and means for providing bank information security: database management systems(distributed databases); data warehouses, OLAP- and OLTP- data processing technologies (online analytical processing systems and online transaction processing systems); search systems, retrieving and preparation of reliable data; distributed computer, organizing the teamwork of users, creation of realistic bank information space, including branches, customers and partners; safe connection of bank information system to external computer networks (Internet); organizing safe, reliable data transmission through overt channel (cryptography: encryption and digital signature (DS), organizational measures), electronic workflow; technical, software, mathematical and other support; information analytics and decision support systems (*DSS*); protection of stored and processed information as well as the whole ABS; remote working systems for stock markets and course behavior forecasting programs; customer relation management systems (*CRM*); implementing programs for interconnection between front-office and customers; organization support, management and personnel executive activity systems; access control to information of different secrecy level; antivirus protection; e-shops and e-cards; call processing centers (*call*-centers), IP-telephony; maintenance of different access channels: Internet, phone, mobile network, *SMS*, *WAP* and so on; supporting of different accounting standards, including managerial accounting; supporting in research in the sphere of systematic informational development of ABS.

Refinement and complement of set of actual bank information security threats with from the triune position of providing information security, security of information and cyber security in bank sphere as a basis for creating new synergetic approach in the field of ABS information security

To achieve the desired goal and find the necessary and sufficient conditions, which provide the synergetic effect in security sphere of state and private bank security systems, we will analyze and define set of actual bank security threats. But before it should be stated that for the first time in the framework of bank information security are put the principles of synergetic. The interaction profiles, ensuring security of bank information should be considered as security of information, information security and cyber security, which till now had been considering separately, or in combination, it was impossible to obtain a synergetic effect in bank information security. After decomposition of certain security profiles consider them separately in order to determine the most relevant threats. According to [9] and further the bank security threat means random or targeted, potential or real activities with different nature capable of inflicting damage to bank.

It is known that for analysis of the main bank information security threats may be used adapted model of CIA triad (*confidentiality, integrity, availability*) [2, 25]. In this model the *security of information* means process of providing confidentiality, integrity, availability of information to/from bank customers based on the totality of the collective and individual consciousness. At the same time the confidentiality means providing access to information only for authorized users, the integrity means providing reliability and completeness of information, its processing methods for authorized

users, the *availability* means providing access to information and associated with it assets for authorized users when needed.

Considering the specificity of bank sector the main threats to the security of bank information, are the following [34]:

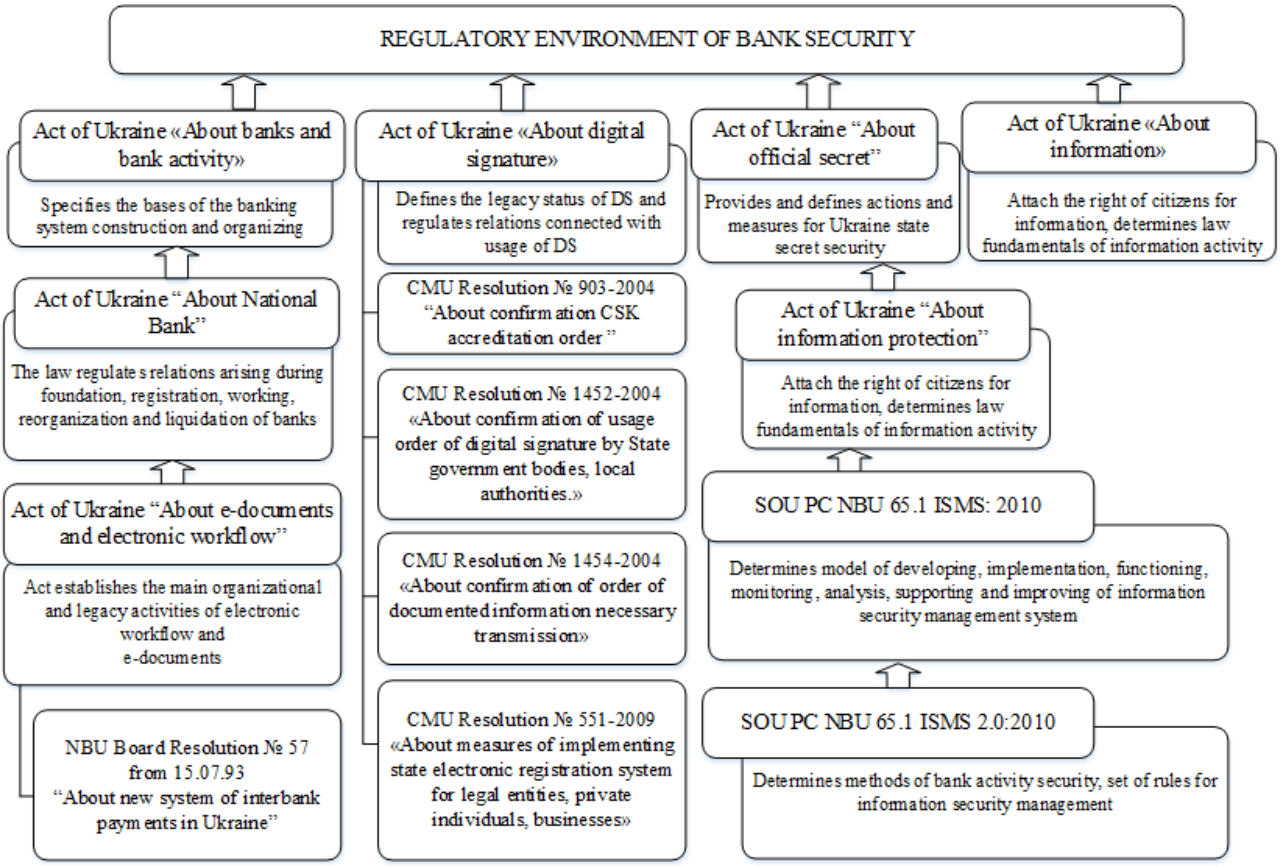

Fig. 2. Current regulatory environment activity of ABS in Ukraine and its interconnections

Breach of confidentiality: user password exposure during undeclared active network connection, traffic analysis for the communication protocols detection, making false allegations of payment documents receiving, unauthorized data input, retrieving information from statistical databases based on semantic connections between public and private information, connection to the CN as an active transponder (payment documents falsification), spoofing, pharming, pretexting, skimming, virtual abducting, unauthorized transmission of confidential data, install hidden radio transmitting equipment in order to copy high-secrecy data or get access to it , covert hardware or software reorganization in order to implement unauthorized access to information resources.

Integrity violation: copying data from magnetic media, leaved on the table or in computer without attendance, copying data from equipment and magnetic media, tucked away in special storage facilities, use of implemented in system terminal, leaved without control, software copying and hijacking, changes in the data and programs for the financial documents forgery and falsification as a result of secret visits after working hours, retrieving information from hard and floppy disks, making changes in an unattended recorded data, use the software to overcome the system defensive capabilities, unauthorized use of computer resources, destruction of equipment, magnetic media, or remote data destruction, modification or reading the information in the database or separate files through the assignment of other people's powers to modify financial information, replacement equipment elements left unattended during business hours.

Availability (authenticity) violation: unauthorized use of high-secrecy level information, exceeding of authority to access, bypassing security mechanisms, the subscriber denial from the fact of reception (transmission) or creating false information about the reception(transmission) time of messages to absolve themselves of responsibility for the execution of these operations, penetration into the system through the communication CN with the assignment of powers for the purpose of information counterfeiting, copying or theft, an abuse of supervisor privileges in case of violation bank information protection mechanisms, identification of passwords during the abduction or visual observation, just the disclosure and modification of data.

Among the threats to bank information security that significantly affect the bank, bank staff and its clients, as well as on the economic component of national security are the internal and external threats. Both the first and second by the direction and nature of the impact on the certain subjects and objects activities can be economical, physical and intellectual [29, 30].

Economical threats: corruption, fraud, unfair competition, using by banks unworkable technologies of bank production. The implementation of these threats leads to causing losses to banks or omission corresponding benefits.

Physical threats: thefts, stealing of property and bank assets, breakdowns, bank equipment lay-up, inefficient exploitation of forces and resources. As a result of these threats realization are inflicted losses to bank associated with loss of their property and the need to carry additional costs for restore the production means and other tangible assets.

Intellectual threats: disclosure or misuse of bank information, bank discreditation on bank services market, different social conflicts about banking institution or in it. The consequences of the implementation of such threats are: bank losses, reputation deterioration, social or psychological tension around the banking institutions or in their teams.

The third essential safety profile of bank information is proposed to be cyber security. *Cyber security* - a set of tools, policies, security principles, security guarantees, risk management approaches, actions, training, insurance and technology, which are used to protect the cyber environment, organization resources and users [14, 16, 29]. According to the standard, *ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity* on cybersecurity are also assigned the tasks for providing the conditions of achieving and preserving the security properties of the organization's resources or users directed against the corresponding cyber threats. At the same time cyber security covers such things as the protection of personal information and interacts with network security, application security, Internet security and security of critical information infrastructures (Fig. 3).

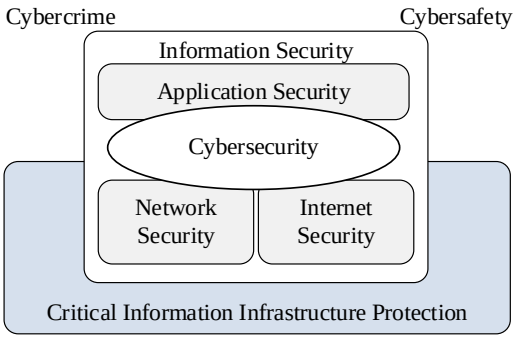

Fig. 3. Logical relationships between cyber security and other security domains according to the standard *ISO/IEC 27032:2012*

Analysis of results in the assessment the cyber attacks number, including ABS attacks, the ratio between the levels of software complexity and technical intruders literacy derived by such companies as "Arbor Networks" [32], Cisco [33] and other vendors in the cyber security market and means network periphery, leads to the conclusion that with the growth of cybercrime and computing capabilities in the near future we should expect an increase not only of the quantity and technical complexity of cyber attacks, but also their refocusing on the peripheral network equipment. Considering this, and basing on results of studies [2, 4, 5, 26 - 28, 32, 33], it can be stated that the main threats to ABS cybersecurity directed at disrupting the control processes or to control them will be a cyber attack which may be grouped into four main classes, a substantial part of which is disclosed at Fig.4.

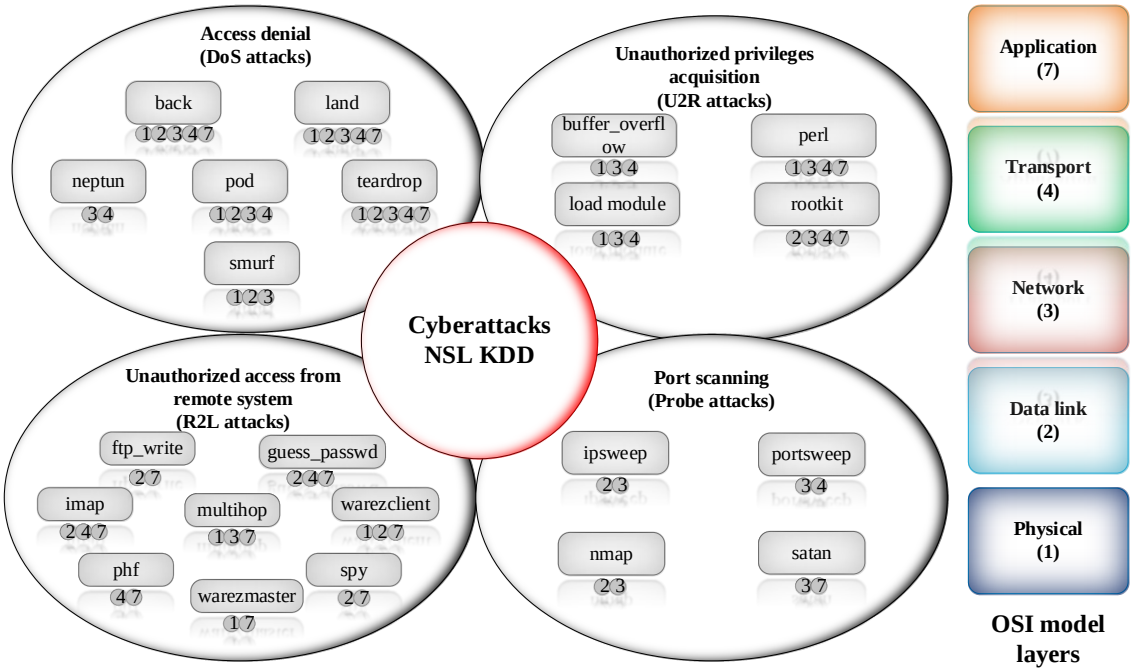

Fig. 4. ABS cyberattacks classification divided by *OSI* model layers

The proposed classification (see. Fig. 4) demonstrates that cyber attacks of different classes regardless on the functional purpose take place at different layers of the OSI(Open System Interconnection) model, and consequently have their own specific objectives for the impact on bank information. For example, before cybercriminals through the protocols and services vulnerability of the lower OSI model layer opens the possibility of obtaining technological bank information, and through the

vulnerability of the upper levels - the organizational and parametric bank information.

Considering that threat described above and due to various subjective and objective reasons have had and will continue to have place for most of the known or designed ABS, based on the t close relationships between them for different security profiles, and, in order to develop an effective system of protection of bank information, is proposed a new model of bank information security threats further named the synergetic (Fig. 5).

The feature of the proposed model (see. Fig. 5) is displayed on it in the form of logical connections between risk interactions for different security profiles. Thus the synergetic model of bank information security threats is laid the necessary and sufficient conditions for the development of a new methodology aimed at achieving synergies in the field of protection security of public and private bank systems.

In a base of a developed synergetic model (see Fig. 5) are also becomes clear mechanism of bank information security problems origin in the space-time continuum: the goal of cybercriminals (competitors, cyber terrorists, individual states, etc.) are coordinated with time, place, problems, objectives and forms of implementation.

Taking into account the features of construction means of network peripheral [1, 3–5, 9, 14, 18–20, 25] and organizational communications in ABS of any bank, the synergetic model allows to define the most vulnerable places in their security system. These are processes associated with transfer of payment and other messages between banks (business process / business products), between bank and ATM, between bank and client. As a result are raised a number of system problems: problems of establishing mutual authentication during performing connection (mutual recognition of subscribers); problems of ensuring the confidentiality and integrity of documents (protection of electronic documents transmitted via communication channels); problems of proving the fact of document delivery or receiving (protection of electronic document exchange process); problems of mutual distrust between the sender and the recipient due to their belonging to different organizations and mutual independence (ensuring the execution of documents).

An essential part of bank information security problem is a risk analysis problem. In fact, the risk is an integrated evaluation of how effectively existing means of protection are capable to resist the attacks on bank information. For today it is possible to single out two main groups of security risk assessment methods. As applied to bank sector on the basis of the first group it is possible to set the level of risk by estimating degree of compliance to a particular set of requirements for ensuring bank information security. The second group of methods for risk estimation defines the probability of attacks, as well as levels of damage. In this case, the risk value is calculated separately for each attack and is generally represented as multiplication of attack probability on the amount of possible attack damage. The value of damage is determined by the owner of bank information; the probability of an attack is calculated by the expert group, performing the audit procedure.

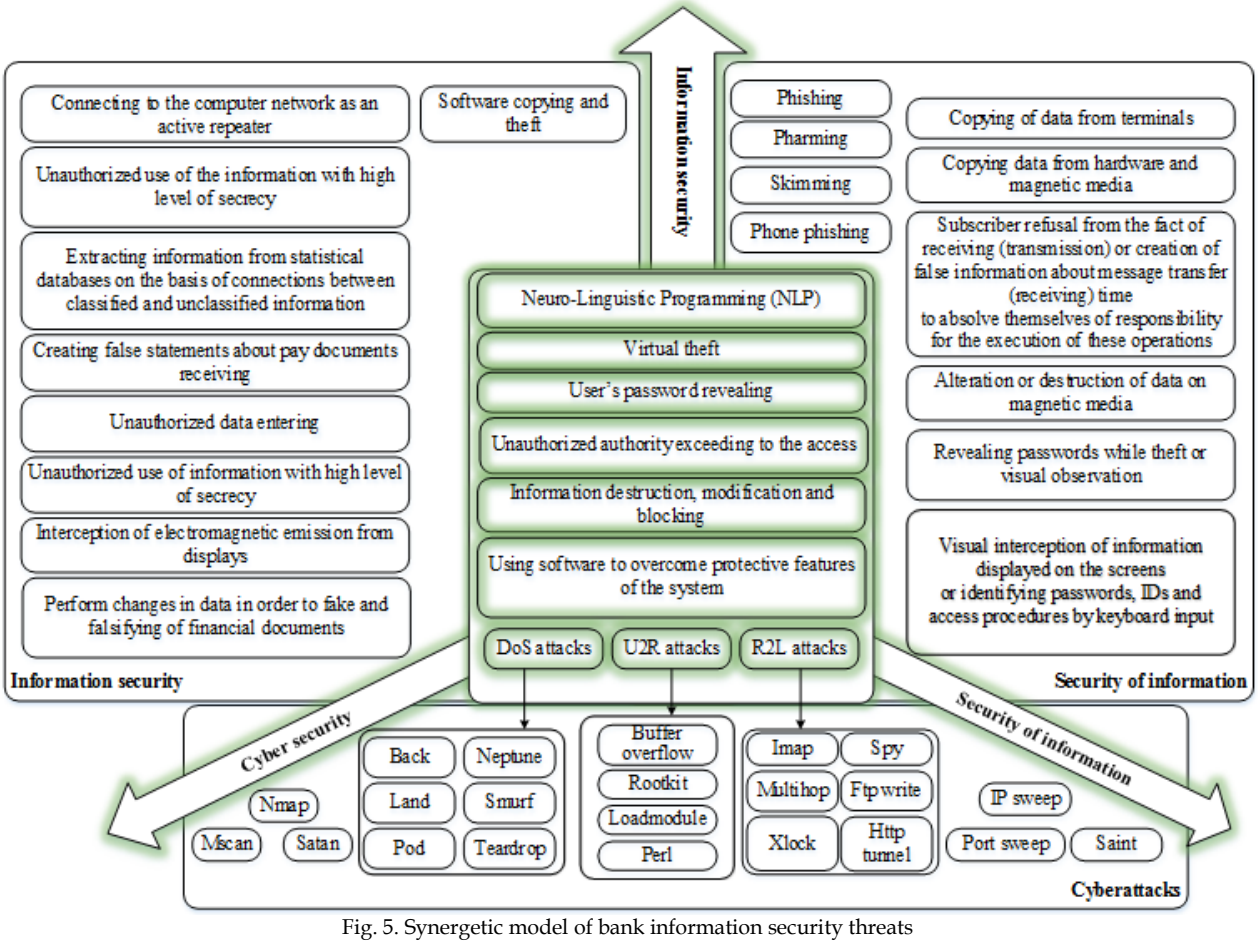

Fig. 5. Synergetic model of bank information security threats

Formalization of the security problem essence and content of bank information on the basis of proposed synergetic approach

Thus, based on the requirements of compliance with the rules of the triune position to ensure the safety of bank information as part of the synergetic approach in the interaction between the selected security profiles and to increase its level of protection assessed risk value equivalent money-capital, the meaning of the proposed approach in the most general form can be represented as some conditional figure (Fig. 6).

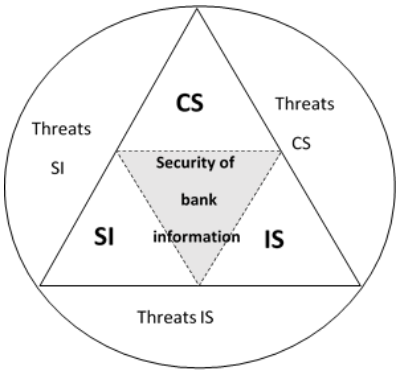

Fig. 6. Synergetic approach essence for providing security of bank information *ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity*

It should be noted that the key feature characteristic offered only for a synergistic approach to bank information security: the proposed approach is not a simple aggregation of the forces and means of security, and it isn't a superposition of their properties. **The main aim of the proposed approach - the excitation of managed emergent properties in bank information system to obtain the synergetic effect, which is achieved due to a qualitatively new approach to security.** The development of such an approach is inconceivable without developing a unified methodology for the bank information security system , which is based on a problem deep scientific elaboration through its comprehensive critical analysis and the synthesis of new non-trivial solutions, based on these conclusions. Today, as the analysis shown, both in theory and practice of bank information security such methodology is absent.

Considering the different nature of threats to selected profiles of bank safety and in order to obtain amount of risk assessments just displaying its security, in the future, equivalent to money-capital, is also proposed to introduce the synergetic safety indicators of bank information in ABS (Fig. 7). *The synergetic safety indicator of bank information in ABS* means synergetic evaluation of the effectiveness of complex forces usage and means of bank information security in an antagonistic conditions of counteraction of bank protection system to random or targeted security threats.

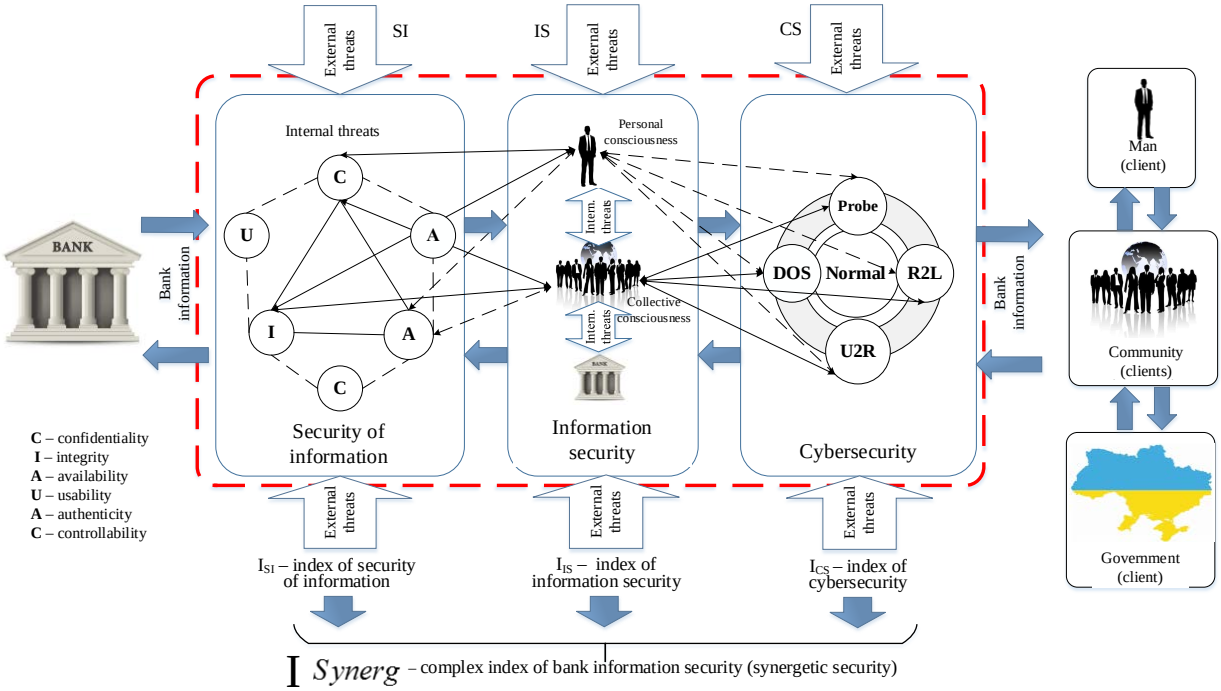

Fig. 7. The role and place of bank information security synergetic index in modern protection automated bank systems

Lack of an appropriate methodology to date is also possible due to the presence of contradictions, which is determined by the fact that on the one hand the practice requires a theory of finding new approaches to security of bank information in a growing number of threats to its cyber- and information security, and information security with a simultaneous increasing of their technological difficulties. On the other hand, in theory there is no integral science-based methodology for the practice of the bank information security system as a whole, due to the imperfection of the mechanism ensuring its information security, security of information and cyber security in particular (Fig. 8) [13–16, 22, 23].

Based on the nature of scientific problem (see. Fig. 8) in general it can be stated as follows.

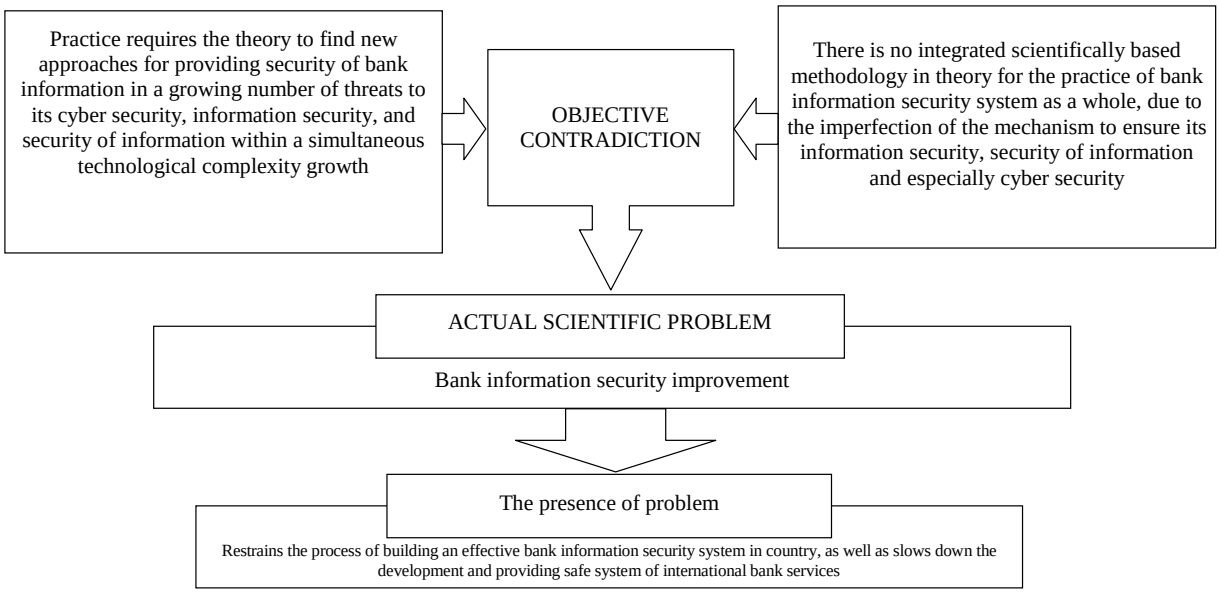

Fig. 8. The essence of scientific problem

Consider that created system for providing bank security consisting of M basic safety profiles of different complexity and configuration, each of which in turn consists of m safety elements in a single security profile, aimed at obtaining synergetic effect - increase the level of banking information security by maximizing the number of its emergent properties

$$Emerdg = max\left\{ I_{Synerg\,N}^{\;M} \right\},$$

where $I_{Synerg\,N}^{\;M}$ – the maximum number of emergent properties of bank security system as a whole, achieved at occurrence of synergetic effect due to the interaction of selected security profiles, N – the number of system states for providing bank information security or number of its emergent properties, $M \le N$.

The maximum number of emergent properties of bank security system as a whole is achievable if the following condition $I_{Synerg\,N}^{\;M} = \sum_{m=1}^{M} C_N^m$ is true.

It is also necessary to solve the problem of increasing the level of bank information security under specified conditions, to get the maximum number of emergent properties at minimal resource cost, aimed at inciting synergetic effect in the system.

Conclusions

Thus, the article in general formalized problem essence of increasing the level of bank information security on the basis of its comprehensive critical analysis and synthesis of new solutions. As a new progressive solution of existing problem was proposed a principally new synergetic approach, which up to now has not been applied at the protection of bank information systems. This fact not only determines the relevance of the research topic, but also its scientific priority.

It is formulated hypothesis that indefeasible interaction profiles for providing bank information security, leading to the emergence of synergetic effect and, as a consequence, the manifestation of emergent properties in the protection system, at the present stage of science and technology development must be information security, security of information and cyber security.

On the basis of considered approach it is at first proposed the synergetic model of bank information security threats, disclosed the role and place of bank information synergetic security index in modern systems of bank protection and automated bank systems.

The obtained in the article results can be used to solve particular scientific problems within the formulated conditions.

Perspective direction for further research is to study of security profiles nature and content which make up a system of bank information protection.

References

[1] Himka S.S. Razrabotka modelej i metodov dlya sozdaniya sistemy informacionnoj bezopasnosti korporativnoj seti predpriyatiya s uchetom razlichnyh kriteriev / S.S. Himka. (Online): http://masters.donntu.org/2009/fvti/khimka/diss/index.htm.

[2] Ukrainskij resurs po bezopasnosti (Online): http://kiev-security.org.ua.

[3] Slobodenyuk D. Bankovskie tekhnologii, Sredstva zashchity informacii v bankovskih sistemah / D. Slobodenyuk. – 2013. – (Online): http://www.arinteg.ru/about/publications/press/sredstva-zashchity-informatsii-v-bankovskikh-sistemakh-131107.html.

[4] Simakov M. N. V S'ezd direktorov po informacionnoj bezopasnosti / M. N. Simakov. – Moskva, 2012. – (Online): http://www.cso-summit.ru/data/2012/presentations/cso2012_013_express-tula_simakov.pdf.

[5] Revenkov P. V. Zashchita informacii v banke: osnovnye ugrozy i bor'ba s nimi / P. V. Revenkov. – (Online): http://www.crmdaily.ru/novosti-rynka-crm/

568-zashhita-informacii-v-banke-osnovnye-ugrozy-i-borba-s-nimi.html.

[6] Security of Internet Banking - A Comparative Study of Security Risks and Legal Protection in Internet Banking in Thailand and Germany (Online): http://www.thailawforum.com/articles/internet-banking-thailand.html.

[7] Yarochkin V. I. Informacionnaya bezopasnost' [Tekst]: uchebnik / V. I. Yarochkin; 2-e izd. – M. : Akademicheskij Proekt; Gaudeamus, 2004. – 544 p.

[8] Starinskij M.V. Shchodo viznachennya ponyattya "bankivska informaciya" ta vidilennya її vidiv (Online): uabs.edu.ua/images/.../K.../Starinskii_s_015.pdf.

[9] Yevseiev S. Analiz zakonodatelnoj bazy k sisteme upravleniya infor-macionnoj bezopasnostyu NSMEHP / S. Yevseiev, O. Korol, H.Kotz. // Vostochno-evropejskij zhurnal peredovyh tekhnologij. – Kharkov. – 2015. – Vyp. 5/3(77). – p. 48-59.

[10] Yevseiev S. Two-factor authentication methods threats analysis/ S. Yevseiev, B. Tomashevskyy // RadIoelektronIka, Informatika, upravlInnya. – ZaporIzhzhya. – 2015. – Vip. 1(32). – p. 52–60.

[11] Serdyuk V. A. Novoe v zashchite ot vzloma korporativnyh sistem. – M. : Tekhnosfera, 2007. – 360 p.

[12] Банківська безпека: Підручник / Корченко А.О., Скачек Л.М., Хорошко В.О. / За заг. ред. докт. техн. наук, проф. О.В.Хорошка. – К.: ПВП «Задруга», 2014 – 185 с.

[13] Грищук Р. В. Синтез систем інформаційної безпеки за заданими властивостями / Р.В. Грищук // Вісник національного університету "Львівська політехніка". – 2012. – № 741. – С. 271–276.

[14] Грищук Р. В. Атаки на інформацію в інформаційно-комунікаційних системах / Р. В. Грищук // Сучасна спец. техніка. – 2011. – № 1 (24). – С. 61–66.

[15] Грищук Р. В. Синергія інформаційних та кібернетичних дій / Р. В.Грищук, Ю. Г. Даник // Труди університету. – К. : НУОУ, 2014. – № 6 (127). – С. 132–143.

[16] Грищук Р. В. Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак / Р. В. Грищук, В. В. Охрімчук // Безпека інформації – 2015. – Т. 21. – № 3. – С. 276–282.

[17] Бурячок В.Л. Політика інформаційної безпеки [Текст] : підручник / В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко ; під заг. ред. проф. В. О. Хорошка. – К. : ПВП «Задруга», 2014. – 222 с.

[18] Даник Ю.Г. Основи захисту інформації [Текст] : навч. пос. / Ю. Г. Даник, С. Г. Вдовенко, В.І. Шестаков, О.О. Писарчук, Р.В. Грищук, М.В. Куликівський, В. М. Ходаківський. – Житомир : ЖВІ ДУТ, 2015. – 220 с.

[19] Даник Ю.Г. Синергетичні ефекти в площині інформаційного та кібернетичного протиборства / Ю. Г. Даник, Р. В. Грищук // Наук.-практ. конф. [«Актуальні проблеми управління інформаційною безпекою держави»] (Київ, 19 берез. 2015 р.). – К. : Центр. навч., наук. та період. видань НА СБ України, 2015. – С. 235–237.

[20] Грищук Р. В. Напрямки підвищення захищеності комп'ютерних систем та мереж від кібератак / Р.В. Грищук, В.В. Охрімчук // II Міжнар. наук.-практ. конф. ["Актуальні питання забезпечення кібербезпеки та захисту інформації"] (Закарпатська область, Міжгірський район, село Верхнє Студене, 24-27 лют. 2016 р.). – К. : Видавництво Європейського університету, 2016. – С. 60–61.

[21] Rodzhers, Everett M. Difuziya innovatsiy [per. z angl.] / Everett M. Rodzhers – Vid. dim «KiEvo-Mogilyanska akademiya», 2009. – 591 p.

[22] Kolesnikov A. A. Sinergeticheskoe metodyi upravleniya slozhnyimi sistemami : teoriya sistemnogo sinteza / A. A. Kolesnikov. – M. : Editoral URSS, 2005. – 228 p.

[23] Haken G. Sinergetika. ierarhiya neustoychivostey v samoorganizuyuschihsya sistemah i ustroystvah / G. Haken. – M. : Mir, 1985. – 419 p.

[24] Serikov A. V. Effektivnost hozyaystvennoy deyatelnosti : opredelenie, izmerenie, sinergeticheskoe upravlenie / A. V. Serikov // Ekonomichniy visnik Donbasu. – 2011. – # 2 (24). – p. 212–219.

[25] Olifer, V. G. Bezopasnost kompyuternyih setey / V. G. Olifer, N. A. Olifer. – M. : Goryachaya liniya – Telekom, 2015. – 644 p.

[26] CERT-UA report 2010-2013. – 2014 (Online): http://cert.gov.ua/?p=316.

[27] Kiberschit Ukrainyi: kto stoit na strazhe kibergranits stranyi [Elektronniy resurs]. – 2015 (Online): http://zillya.ua/ru/kibershchit-ukrainy-kto-stoit-na-strazhe-kibergranits-strany.

[28] Ten C.-W. Cybersecurity for critical infrastructures : Attack and defense modeling / C.-W. Ten, G. Manimaran, C.-C. Liu // IEEETrans. Syst., Man Cybern. A, 2010, - vol. 40, no. 4, pp. 853 -865.

[29] Lenkov S.V. Metody i sredstva zashchity informacii : monografiya [v 2-h t.] T. 2. Informacionnaya bezopasnost' / S. V. Lenkov, D. A. Peregudov, V. A. Horoshko. – K. : Arij,2008. – 344 p.

[30] Yudin O.K. Informacijna bezpeka. Normativno-pravove zabezpechennya / O. K. Yudin. – K. : NAU,2011. – 640 p.

[31] Metodichni rekomendacії shchodo vprovadzhennya sistemi upravlinnya informacijnoyu bezpekoyu ta metodiki ocinki rizikiv vidpovidno do standartiv nacional'nogo banku Ukraïni (Online): zakon.rada.gov.ua/laws/show/v0365500-11

[32] Worldwide Infrastructure Security Report. 2014. Arbor Networks, Inc Електронний ресурс: 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.

[33] Bezopasnost' IP-setej novogo pokoleniya dlya provajderov uslug (Online): http://www.eureca.ru/edu/study/cisco/library/download.php?type=pdf&att=IP_NGN.pdf.

[34] Yevseiev S. Analiz zashchity v nacional'noj sisteme masovyh ehlektronnyh platezhej // Informacijna bezpeka.– 2014. – № 3(15), № 4 (16) – P. 15-28.

УДК 004.056.53:336.719.2 (045)

Грищук Р. В., Євсєєв С. П. Синергетичний підхід до забезпечення безпеки банківської інформації: постановка проблеми.

Анотація. *Постійно зростаюча кількість загроз безпеці банківської інформації в автоматизованих банківських системах (АБС) призводить до зниження якості послуг, що надаються банками на національному та міжнародному рівні незалежно від їх форми власності. Ситуація, що склалася не в останню чергу обумовлена недосконалістю застосовуваних сьогодні механізмів забезпечення безпеки банківської інформації. Технологічна складність виявлення нових невідомих загроз безпеки, а також наростаюча витонченість в методах їх реалізації обумовлює нагальну потребу кардинального перегляду існуючих підходів до її забезпечення. Існуючі підходи як відомо в основному орієнтуються на комплексування сил і засобів забезпечення безпеки банківської інформації, що часто призводить до неповного перекриття спектру загроз і нераціонального використання ресурсів, виділених на забезпечення безпеки. Таким чином, стає зрозуміло, що розробка принципово нового підходу до забезпечення безпеки банківської інформації, якому і присвячена ця стаття, є необхідною умовою надання якісних банківських послуг. З цією метою в статті запропонована синергетична модель загроз безпеки банківської інформації, яка вперше з системних позицій дозволила розкрити сучасний стан досліджуваної проблеми. Показано і доведено, що на сучасному етапі розвитку науки і техніки, забезпечення безпеки банківської інформації повинно ґрунтуватися на принципово новому підході, який запропоновано називати синергетичним. Його впровадження дозволить отримати синергетичний ефект при взаємодії обраних профілів безпеки і, як наслідок, проявити якісно нові і невідомі до цього емерджентні властивості системи безпеки. У рамках запропонованого підходу в загальному вигляді формалізована проблема підвищення рівня захищеності банківської інформації та визначені подальші шляхи її вирішення. Показано, що відсутність подібних рішень в системах забезпечення банківської інформації визначає актуальність обраної теми для дослідження і її науковий пріоритет.*

Ключові слова: *автоматизована банківська система, банківська інформація, безпека інформації, інформаційна безпека, кібербезпека, синергетична модель загроз безпеці, синергетичний показник безпеки, емерджентність.*

Грищук Р.В., Евсеев С.П. Синергетический подход к обеспечению безопасности банковской информации: постановка проблемы.

Аннотация. *Постоянно возрастающее количество угроз безопасности банковской информации в автоматизированных банковских системах (АБС) приводит к снижению качества банковских услуг, предоставляемых банками на национальном и международном уровне независимо от их формы собственности. Сложившаяся ситуация не в последнюю очередь обусловлена несовершенством применяемых сегодня механизмов обеспечения безопасности банковской информации. Технологическая сложность выявления новых неизвестных угроз безопасности, а также нарастающая изощрённость в методах их реализации обуславливает насущную необходимость кардинального пересмотра существующих подходов к ее обеспечению. Существующие подходы как известно в основном ориентируются на комплексирование сил и средств обеспечения безопасности банковской информации, что зачастую приводит к неполному перекрытию спектра угроз и нерациональному использованию ресурсов, выделенных на обеспечение безопасности. Таким образом, становиться понятно, что разработка принципиально нового подхода к обеспечению безопасности банковской информации, которому и посвящена эта статья, является необходимым условием предоставления качественных банковских услуг. С этой целью в статье предложена синергетическая модель угроз безопасности банковской информации, которая впервые с системных позиций позволила раскрыть современное состояние исследуемой проблемы. Показано и доказано, что на современном этапе развития науки и техники, обеспечение безопасности банковской информации должно основываться на принципиально новом подходе, который предложено называть синергетическим. Его внедрение позволит получить синергетический эффект при взаимодействии выбранных профилей безопасности и, как следствие, проявить качественно новые и неизвестные до этого эмерджентные свойства системы безопасности. В рамках предложенного подхода в общем виде формализована проблема повышения уровня защищенности банковской информации и определены дальнейшие пути ее решения. Показано, что отсутствие подобных решений в системах обеспечения банковской информации определяет актуальность выбранной темы для исследования и ее научный приоритет.*

Ключевые слова: *автоматизированная банковская система, банковская информация, безопасность информации, информационная безопасность, кибербезопасность, синергетическая модель угроз безопасности, синергетический показатель безопасности, эмерджентность.*

Отримано *18 лютого 2016 року*, затверджено редколегією *2 березня 2016 року*