Розвиток обчислювальних засобів і технологій корпоративних мереж розширило спектр освітніх та інформаційних послуг в корпоративних науково-освітніх мережах (КНОС). Такі мережі відносяться до критичних кібернетичних інформаційних систем (ККІС), побудованих на основі моделей відкритих мереж. Такий підхід на початку 80-х років XX ст. не розглядав необхідність побудови системи безпеки, що не дозволяє забезпечити певний рівень безпеки від сучасних гібридних загроз. Перехід на автономність управління університетами в усьому світі висуває вимоги до забезпечення необхідної якості обслуговування (QoS) клієнтів КНОС. До користувачів КНОС відносяться адміністрація університету, професорсько-викладацький склад, студенти та персонал, який обслуговує освітняні процеси в ЗВО. Одним з головних критеріїв QoS є безпека інформації. Однак загального підходу до побудови комплексного захисту інформації в КНОС, яка забезпечувала необхідний рівень безпеки немає.

В основу методології запропонована концепція синтезу синергетичної моделі загроз на ККІС, удосконалених моделей інфраструктури КНОС, порушника, оцінки поточного стану інформаційної безпеки (ІБ) і вдосконаленого методу інвестицій в ІБ КНОС. Показано, що базис синергетичної моделі становить трирівнева модель стратегічного управління безпекою, яка забезпечує отримання синергетичного ефекту в умовах одночасної дії загроз інформаційній безпеці, кібербезпеці та безпеці інформації. На відміну від відомих такий підхід забезпечує визначення якісно нових і невідомих до цього емерджентних властивостей системи безпеки інформації з урахуванням коштів використаних на її створення. Застосування методології на практиці за рахунок розробки та впровадження нових рішень забезпечення послуг безпеки дозволяє забезпечити необхідний рівень безпеки інформації в КНОС. Запропоновані механізми послуг безпеки інформації будуються на гібридних криптосистемах на основі крипто-кодових конструкцій зі збитковими кодами

Ключові слова: корпоративна науково-освітня система, класифікатор загроз безпеки, система забезпечення інформаційної безпеки

UDC 681.32:007.5
DOI: 10.15587/1729-4061.2019.169527

DEVELOPMENT OF A METHODOLOGY FOR BUILDING AN INFORMATION SECURITY SYSTEM IN THE CORPORATE RESEARCH AND EDUCATION SYSTEM IN THE CONTEXT OF UNIVERSITY AUTONOMY

S. Yevseiev
Doctor of Technical Sciences, Senior Researcher*
E-mail: serhii.yevseiev@hneu.net
V. Aleksiyev
Doctor of Technical Sciences, Professor*
S. Balakireva
PhD
Air Force Science Center***
Y. Peleshok
PhD, Deputy Head of the Research Center
Institute of Special Communication and Information Protection
National Technical University of Ukraine «Igor Sikorsky Kiev Polytechnic Institute»
Verkhnokliuchova str., 4, Kyiv, Ukraine, 03056
O. Milov
PhD, Associate Professor*
O. Petrov
PhD
Department of ACS Mathematical and Software Support***
O. Rayevnyeva
Doctor of Economic Sciences, Professor
Department of Economy Theory, Statistics and Forecasting**
B. Tomashevsky
PhD, Associate Professor
Department of Cyber Security
Ternopil Ivan Puluj National Technical University
Ruska str., 56, Ternopil, Ukraine, 46001
I. Tyshyk
PhD
Department of Information Security
Lviv Polytechnic National University
S. Bandery str., 12, Lviv, Ukraine, 79013
O. Shmatko
PhD, Associate Professor
Department of Software Engineering and Information Technology Management
National Technical University «Kharkiv Polytechnic Institute»
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
*Department of Cyber Security and Information Technology**
**Simon Kuznets Kharkiv National University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166
***Ivan Kozhedub Kharkiv National Air Force University
Sumska str., 77/79, Kharkiv, Ukraine, 61023

1. Introduction

In modern conditions, the development of Internet technologies and computing have led to revolutionary changes in the education sector. The unification of information and computer networks of universities formed a unified information and cyber space, which integrated all the components of the enlightened service delivery process, formed corporate

research and education systems (CRES), which significantly expanded the range of education services of universities. As a result, threats to the information resources of CRES were significantly transformed. Threats acquired properties of hybridity. From purely threats to information, cyber security and information security, manifestations of hybrid properties began to take place due to the simultaneous impact on the object of protection – information resources in CRES, due to the emergence of the phenomenon of synergy [1, 2]. A significant drawback of Internet technologies is the use of open systems, which from the very beginning of their development did not provide for the creation of information protection systems. In addition, the dissemination of education and scientific services, the use of CRES for the creation of scientific research, huge personal databases create the conditions for the growth of cyber threats in recent decades. Corporate information and educational systems belong to critical cybernetic information systems (CCIS), based on the principles of open systems (ISO/OSI model), therefore information security in CRES should be considered in the context of general security issues of information systems based on relevant legislation. To objectively assess the current state of information security of the CCIS, it is necessary to consider modern threats to all information security components: information security (IS), cybersecurity (CS) and security of information (SI) [3]. However, there are no relevant documents in the field of education, which does not allow for timely adjusting the security policy of the university. In addition, CRES are used in the autonomy of university management, which imposes additional tasks on the administration in the context of modern hybrid threats.

Under the conditions of autonomy, the institution of higher education (IHE), like any organization, has its own management system, consisting of a set of subjects and objects of management, subsystems and communications between them, as well as processes that ensure the effective functioning of the organization. The organizational autonomy of IHE is not an exception. Thus, the object of management is the internal organizational structure of the IHE and management decisions relating to its changes and made in accordance with the legal framework and statute of the IHE.

The subjects of the management system of IHE organizational autonomy are the bodies and structural units of the IHE involved in the process of formulating the rules for the functioning of the IHE and regulating its organizational structure. In particular, these are the Rector (Head) of the IHE and Deputy Heads (Vice-Rector for Scientific and Pedagogical Work), the Academic Council of the IHE, the Supervisory Council of the IHE, the conference of the labor collective of the IHE and the Legal Department of the IHE. For realization of administrative functions, electronic document management, and high-quality delivery of educational services, CRES should ensure the security of information resources (IR) in the context of the growth of the capabilities of modern threats, the lack of regulatory requirements and legislative acts, and the necessary information security units.

2. Literature review and problem statement

It is known that the methodological basis of any security sector is the key component of the security theory itself and is based on methods and models that are necessary and sufficient to study the problem of security and solve practical problems of the appropriate purpose. So, now in the field of information security there is a fairly large number of methodologies. In particular, the analysis of methodologies that are associated with the development of the scientific basis for the synthesis of the following safety systems is carried out. In [4], for the design of a security methodology, the synthesis and analysis of differential game models and methods for modeling cyber attacks to state information resources are used. However, this approach requires large computational tools in online use. In [5], an assessment of the level of protection of state resources from sociotechnical attacks was developed, but the authors do not take into account the properties of synergy and hybridity of threats, assessment of damage to national security in the field of state secret protection [6]. In [7], the issues of design and applying secure wireless sensor networks with random network parameters were considered, but the specifics of the critical cybernetic information systems to which CRES belongs are not taken into account. In [8], the protection of state information resources is considered, but the authors do not take into account threats to individual security components, the relationship between threats and elements of the CRES infrastructure. The analysis of the complex of technical information protection is considered in [9], the risks of the identifiers tree of state information resources in [10]. In [11], a methodology for constructing systems for detecting anomalies generated by cyber attacks was considered. In [12], there is a methodology for analyzing and assessing the risk of loss of information resources. Comprehensive protection of a person and social groups from negative informational and psychological impact was considered in [13]. The methodology of adaptive risk assessment systems for the security of information system resources is considered in [14]. The analysis of the proposed methodologies in [8–14] showed that the authors use only individual components of information resource security, information security, as a rule, do not take into account the relationship between information assets, elements of the information infrastructure of the corresponding computer networks/systems, the possibility of integration and properties of hybridity of threats to security components [15–17]. Therefore, the reviewed methodologies will require a radical revision in terms of the creation of a methodological basis for building an information security system in CRES both of the world as a whole and of Ukraine in particular.

The methodological principles for security in corporate networks using standard system platforms and operating systems in the context of increasing potential risk for the security of critical infrastructure was discussed in [18]. However, the proposed practical solutions do not take into account the complexion of modern threats, not only among themselves, but also with the use of social engineering methods. This approach does not allow timely response to the modification of threats. The papers [19, 20] consider the methodology for building a security system for critical systems in the context of growing cyber threats to industrial control systems [19] and critical infrastructure [20]. However, the authors do not take into account the hybridity of threats, and consider cyber threats only, which prevents the correction of destructive measures to counter current threats on the SI and elements of information security systems.

In [21], the methodology of preparing the input data set for further analysis using machine learning methods is used to compromise the secret key of the ECC algorithm based

on the risk of information leakage on the processor's side channel. The papers [22, 23] address the issues of security in the conditions of modern cyber threats to objects of cyber-physics systems (CPS) and Internet of things (IoT) at the software level. However, the use of physical channels of information leakage allows access to the resources of these systems. In [24], a methodology for assessing the security for the analysis of the security of critical services deployed in cloud environments is considered. The methodology offers flexibility in the sense that policy-based security assessments can be defined based on user requirements, relevant standards, policies and recommendations. However, the proposed approach does not take into account the hybridity of modern threats, the ability to obtain key data of protection systems through the leak of information on the side channel of hardware processors in cloud environments. In [25], a classifier of modern threats for CPS systems is proposed based on the construction of an attack tree. However, the proposed approach does not take into account the complexity of threats to obtain a synergistic effect when acting on individual security mechanisms.

In [26], research is carried out on factors influencing the awareness of personnel information security, interpretations of cases using several methods of data collection are proposed. In addition, the authors argue that culture and awareness increase the level of security in the corporate network of the university. The paper [27] addresses the lack of relevant legislative acts and educational programs for the establishment of a security system in higher education institution corporate networks. The paper [28] suggests using different types of competitions among IS students, which in turn requires careful preparation for their conduct. However, the measures proposed in the work are aimed at raising the level of information literacy of society and are an addition to the comprehensive information security system (CISS). The paper [29] demonstrates the results of a study on the development of a method and a mathematical model for the authentication of subjects in the electronic informational educational environment of universities (EIEEU). However, the proposed method provides only the service of authenticity, and needs to be «supplemented» with the mechanisms of confidentiality, availability and integrity in the conditions of modern hybrid threats. In [30], a model of the control system of IS for automated critical data processing systems is proposed. The model allows to assess the level of risk for the IS and provides support for decision-making on counteracting unauthorized access to information. However, the model does not take into account the synergy of threats to all security components: IS, CS, SI, so its use does not allow to obtain the emergent properties when using CCIS in CRES.

Based on the analysis [15–32], it can be argued that one of the priority directions of increasing the level of information security in CRES is the design of a security system based on the use of methods and means of protecting information of post-quantum cryptography from hybrid threats to security components: IS, CS, SI.

In [17], the methodology of security building in the banking sector in the context of modern threats synergy is considered, which allows to build a comprehensive information security system that will provide the necessary level of IS. In addition, the approach proposed in [17] is universal and can be used with some refinements for any critical cybernetic system, so let's take this approach as a basis.

Thus, in the conditions of hybridization and integration of threats to security components: IS, CS, SI, there is an objective contradiction between the high requirements of the provision of a certain level of information security in CRES and the imperfection, and sometimes the lack of effective scientifically substantiated methodological principles of its provision.

3. The aim and objectives of the study

The aim of the study is to develop an appropriate methodology for building a system for providing IS in CRES.

To achieve the aim, the following objectives were set:

– to conduct an analysis of the management system of organizational autonomy of the IHE;

– to develop a Concept for building a synergistic model of threats to the security of information resources of the corporate scientific and educational system;

– to formulate the methodology of building a system of information security in the corporate scientific and educational system in conditions of autonomy of the university.

4. Analysis of the control system of university organizational autonomy

Organizational autonomy of the higher education institution is an integral part of institutional autonomy and is intended to create the preconditions for the commercialization of knowledge, the development of internal academic structures, the implementation of strategic management solutions by ensuring the independent creation and functioning of the organizational structure of management of the IHE, the introduction of effective mechanisms for the implementation of management technologies.

The sphere of organizational autonomy covers the formation of general rules for the functioning of the IHE and regulation of its organizational structure, namely: the election, appointment and dismissal of executives and other management bodies of internal structures of IHE; determination of the term of office of directors and signing contracts with them; creation and liquidation of internal structural subdivisions and separate subdivisions of IHE.

The structure of the institutional autonomy management system (IAMS) of the university has the following tuple form:

$$IA^{univ} = \left\langle AA^{univ}, OA^{univ}, HRA^{univ}, FA^{univ} \right\rangle,$$

where IA^{univ} – institutional autonomy of the university; AA^{univ} – academic autonomy; OA^{univ} – organizational autonomy; HR^{univ} – human resource autonomy; FA^{univ} – financial autonomy. The IAMS has a complex structure, which encompasses all organizational units of the university at different levels of management with the complex nature of the relationship between them. Fig. 1 gives a generalized organizational structure of management of the academic autonomy of the IHE.

The analysis of Fig. 1 demonstrated that in order to provide IHE management in an autonomous environment, it is necessary to use the CRES, which should provide the necessary level of quality of services QoS in the conditions of growing demand for the Internet resources of CRES as a whole and its individual subdivisions.

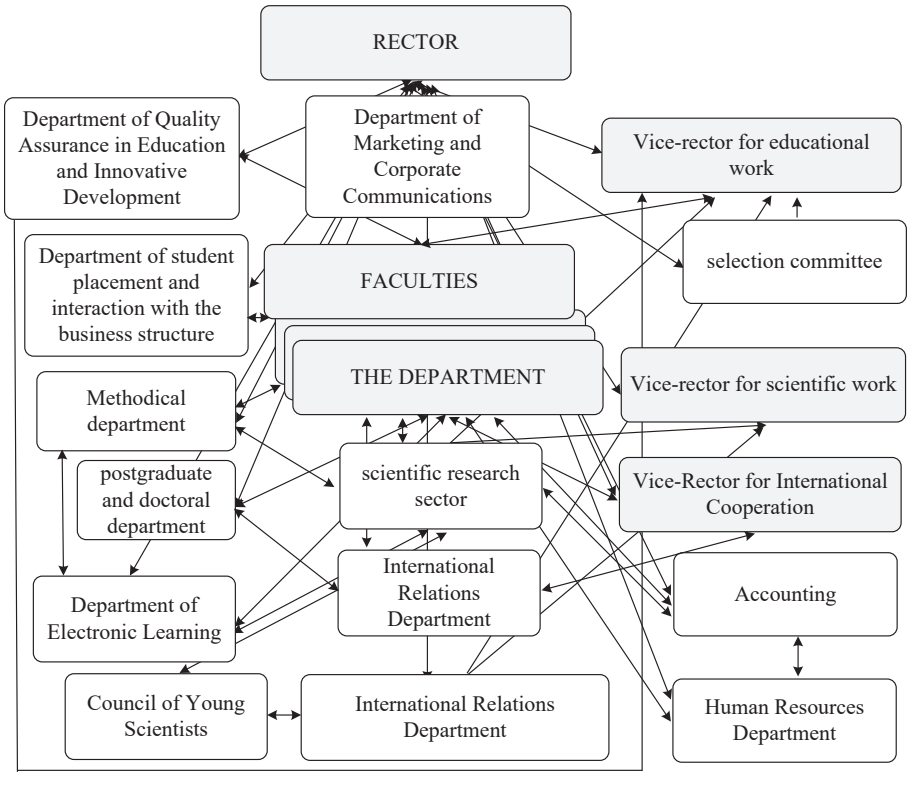

Fig. 1. Generalized organizational structure of management of the academic autonomy of the IHE

Thus, the following principles should be at the heart of the management system of the corporate network of IHE:

– combining the administration of individual functional subsystems (the issue of efficiency can not be solved without considering the issue of network survivability, and safety issues – without taking into account efficiency and survivability (in other words, when changing the level of security, for example, efficiency also changes, which should be taken into account);

– centralized/distributed administration assumes that the main tasks of administration should be solved from the center (the main piece of the network); secondary tasks (for example, within the framework of remote fragments) – by means of managing individual subsystems based on web applications for security of the relevant information resources of CRES;

– within the framework of the management system, the functions of the automatic management system of documentation and autonomy of the IHE on the basis of web applications and the key certification center (KCC) should be implemented. In order to increase the efficiency of response of the control system to particularly important events, the automatic processing of especially important impacts on the CRES elements must be implemented in the system;

– within the framework of the security system, the proposed three-level security model based on the Concept of Strategic Management of Education Services Provisioning in Ukraine's IHE, adaptive security management with an adequate change in relevant events (for example, an attack detection system can block a local port in the event of a «denial of service») should be implemented;

– to improve the efficiency and reliability of the management system, it is necessary to provide an expert system – a system of «prompts» for developing control influences on various events based on artificial intelligence and neural networks.

5. Development of the concept of building a synergistic model of threats to the security of information resources of the corporate scientific and educational system

Social networks are an integral part of the corporate education system (information and education system) of social institutions, the portals of which contain personal data of millions of users, thus representing huge online directories that are available to everyone every day [18, 19]. In today's IHE, a huge amount of different data related not only to the provision of the educational process, but also to research and design developments, personal data of students and employees, service, commercial and other confidential information are stored and processed [33]. However, the conceptual strategy, policies and procedures for ensuring the security of information assets circulating and stored in CRES are not available at the legislative level.

The paper [33] proposes a model of the process of providing educational services, based on a process approach that provides application of the system of processes, together with their definition and interactions, as well as their management in the organization. The advantage of this approach is the continuity of management at the interface of individual processes within the system of autonomy management processes and their combination and interaction. At the same time, post-Soviet bureaucratic state administration remains in Ukraine, which is one of the most important factors of widespread corruption. Based on the functional of the three-level model of the strategic set of a typical enterprise [17] in order to develop the conceptual framework for ensuring the safety of CRES information resources (IR), a concept for constructing a synergistic model of security threats to the CRES IR, based on the three-level security management strategy of the CRES IR and the organizational autonomy management of the IHE is proposed. The *first level* describes the general corporate strategy of the IHE and its functional strategies. The corporate strategy determines the prospects for development and contributes to the implementation of the main IHE mission. At this level, in accordance with the synergistic approach, the general concept of the security of information technology of CRES is considered and the goals and objectives of providing cyber security (CS) are formed, as well as the state of the IR security is determined:

$$S^{KRES}=\left\{S_1^{KRES},S_2^{KRES},...,S_m^{KRES}\right\},$$

where $S_i^{KRES}\in\left\{S^{KRES}\right\}$, $(i=\overline{1,m})$ – the state of security of IR in CRES.

Functional strategies of the same level have horizontal links and are coordinated at the level of goals, with further details at the next level of the strategic set.

At the *second level*, the corporate strategy of IR security is formed:

$$\{RR^{KRES}\}=\{R_{BI}\}\cup\{OV_{BI}\}\cup\{IU_{BI}\},$$

where $\{RR^{KRES}\}$ – a set of regulator requirements that includes IR safety requirements – $\{R_{BI}\}$, as defined in international and national standards; a set of safety performance ratings $\{OV_{BI}\}$ and a set of the previous final level of IR security compliance $\{IU_{BI}\}$. Also the goals and objectives of the main business processes related to the protection of personal data are defined. The corporate security strategy describes how to manage and coordinate efforts with various aspects of security. The strategy is developed in the form of functional strategies: financial economic, physical and information security (IS).

At the *third level*, the functional strategies of the second level of the strategic set are detailed, the corporate strategy of information security is formed. Among the main areas of protection it is advisable to allocate personnel security, physical security, network security and security of information (SI). At this level, the correspondence between the used information protection hardware (IPH) and the threats to IS, CS, SI to the IR security is determined:

$$OPZ^{KRES}=\sum_{i=1}^{k}OPZ_i,$$

where OPZ_i is a generalized indicator of the CRES protection level, which allows to assess the level of compliance of IPH with the requirements of regulators. The IR security strategy is an important management function of the IHE and should be formed by its management based on expert evaluation methods.

For the formation of security services in the autonomy organizational management, taking into account the results of the analysis [33–36], it is suggested to use the proposed Concept of Security in the university's corporate research and educational system on the basis of web technologies. The block diagram of the Concept is shown in Fig. 2. The main elements of a comprehensive security system to provide authentication services of the IHE CRES users and data integrity are the LDAP server and the Key Certification Center.

At the first level, to provide an educational Concept for constructing a synergistic model of security threats to the CRES IR to ensure users authenticity, authorization and identification, it is recommended to use the LDAP server.

To ensure the integrity and authenticity of data at the second level, it is suggested to use the Key Certification Center of the «Code-X.509» system. The ciphertext core of the «Cipher-X.509» system is a software product «Cipher^{+}» (libraries of cryptographic transformations), which has a valid positive expert opinion of the State Service for Special Communications and Information Protection of Ukraine. At the third level of the Concept for constructing a synergistic model of threats to the security of information resources of the corporate scientific and educational network, it is proposed to use software applications to provide antivirus security, attacks on the network and transport levels.

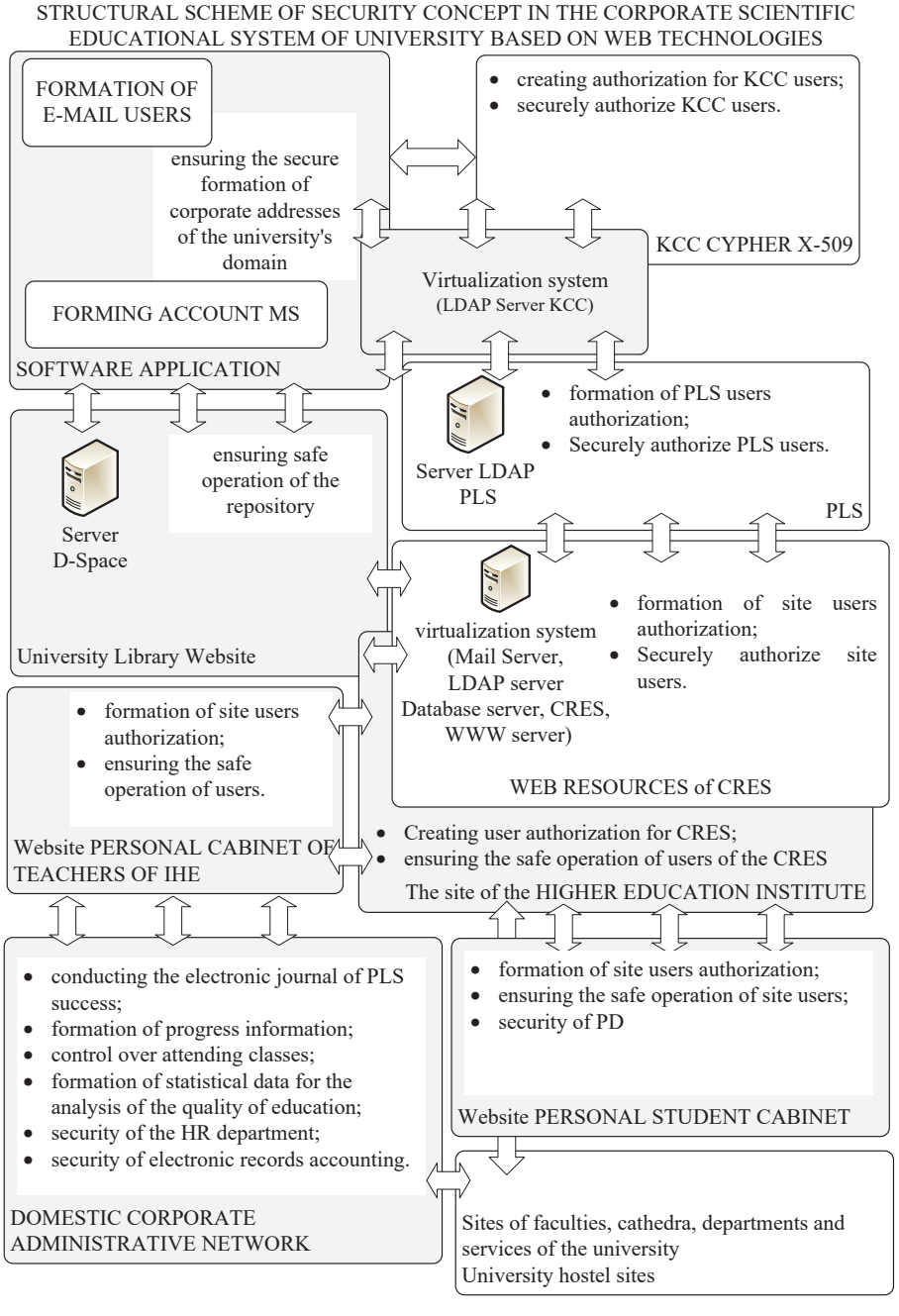

Fig. 2. Block diagram of the Concept of Security in CRES of the University on the basis of web technologies

The proposed concept is based on a synergetic approach to the selection of the most effective directions for achieving the IR safety objectives, taking into account the magnitude of risk at each level of the management model for the IHE organizational autonomy.

6. Formulation of the methodology for building a system of information security in the corporate scientific and educational system in conditions of autonomy of the university

On the basis of the synthesis of the models proposed in [17], we form the methodological principles of constructing the system of maintenance of the IS and assessing the current status of the CRES IS, which are shown in Fig. 3. Relying on the well-known approach to the construction of methodologies [4–14, 18–20, 23, 24], the paper proposes a fundamentally new methodology for constructing a system of maintenance of CRES IR IS. The methodology consists of four stages (Fig. 4–7):

1) determination of the probability of the impact of the threats of IS, CS, SI on the information security of the IR in CRES;

2) determination of the general indicator of the level of IR IS in CRES;

3) assessment of the efficiency of investments in IR in CRES;

4) development of integrated mechanisms for ensuring the confidentiality, integrity, authenticity and credibility of IR in CRES.

The analysis of Fig. 3 demonstrated that the synergetic approach to the evaluation of the efficiency of complex information security means allows the integration of threats, their impact on the elements of the infrastructure and communication lines in CRES, as well as predicting destructive measures to counteract various types of intruders.

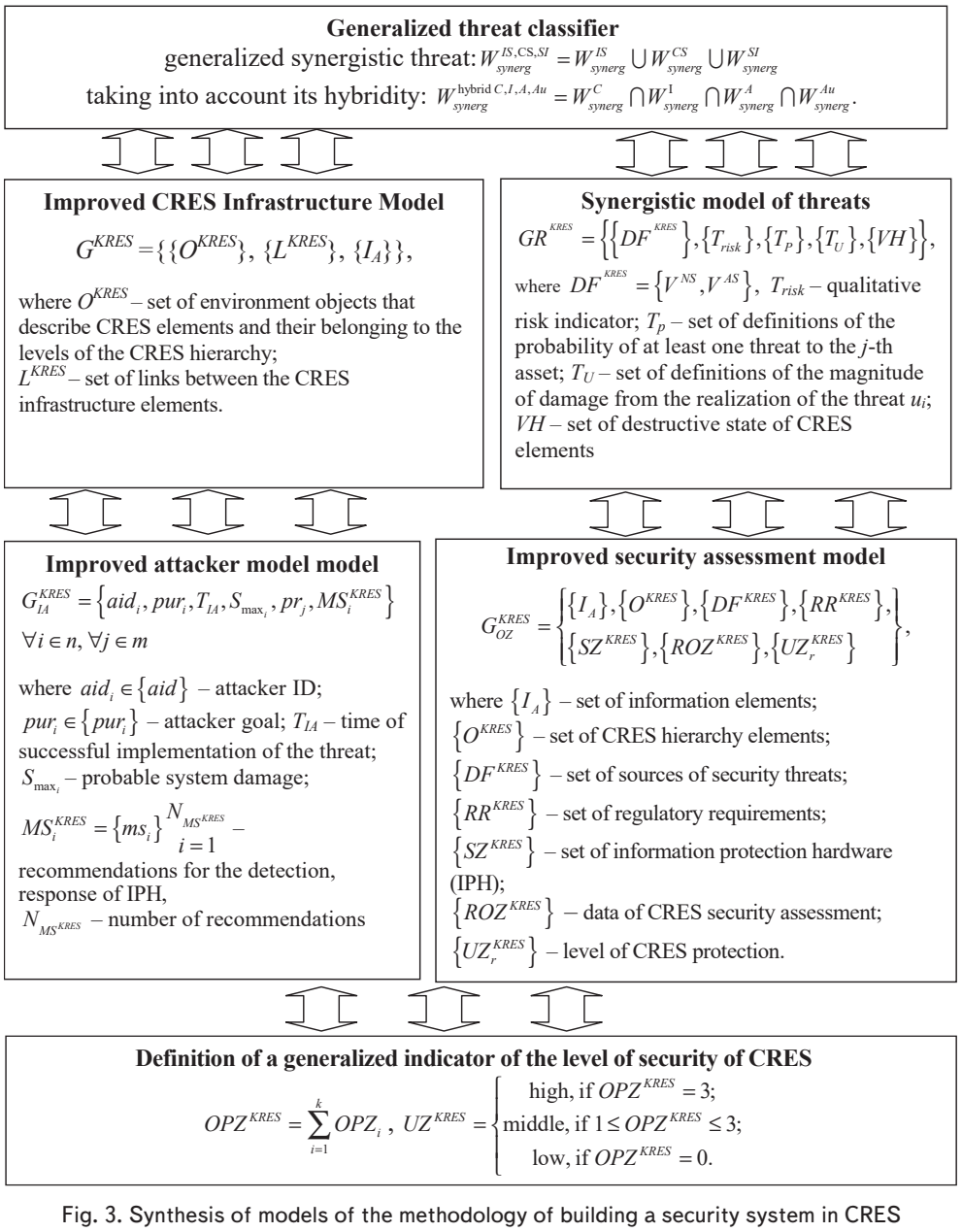

Fig. 3. Synthesis of models of the methodology of building a security system in CRES

Stage 1. Determination of the probability of the impact of threats to IS, CS, IS on the IR security based on the threat classifier.

Step 1. 1. Formation of metric coefficients of threats by experts for security services $w^j = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ik}^j$, where w_{ik}^j – the value of the metric coefficient proposed by the k-th expert for the i-th threat of the j-th security service; N – number of threats; K – number of experts

Step 1. 2. Formation of threat IDs according to the classifier components

Step 1. 3. Selection of the weight coefficients α_i determining the appearance of the i-th threat

Step 1. 4. Determination of the implementation of each i-th threat, taking into account the probability of attack: $w_i^j P_i^j = \frac{1}{K} P_i^j \sum_{k=1}^{N} w_{ik}^j$.

Step 1. 5. Determination of the implementation of the occurrence of several threats to the selected service: $W_{synerg}^{C} = \sum_{i=1}^{M} w_i^C \alpha_i^C$, $W_{synerg}^{I} = \sum_{i=1}^{M} w_i^I \alpha_i^I$, $W_{synerg}^{A} = \sum_{i=1}^{M} w_i^A \alpha_i^A$, $W_{synerg}^{Au} = \sum_{i=1}^{M} w_i^{Au} \alpha_i^{Au}$

Step 1. 6. Determination of the total threat to security components:

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

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

Step 1. 7. Determination of the generalized synergistic threat on IR:

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

Step 1. 8. Determination of the generalized synergistic threat taking into account its hybridity: $W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^{C} \cap W_{synerg}^{1} \cap W_{synerg}^{A} \cap W_{synerg}^{Au}$.

Fig. 4. Stage 1. Determination of the probability of impact of threats of IS, CS, SI on the safety of IR based on the classification of threats

services with one mechanism. Such mechanisms include McEliece and Niederreiter crypto-code systems, which allow to provide confidentiality and integrity of information on the basis of an asymmetric cryptosystem, noise immunity through the use of noise immunity codes, and the speed of cryptographic transitions at the level of the speed of symmetric block ciphers.

In the fourth stage, hybrid crypto-code systems are used based on flawed codes, which are considered in the papers [37, 38].

The use of hybrid crypto-code systems on flawed codes allows you to increase the number of tokens of the authenticator, use two asymmetric crypto-code systems, two/four channels for transferring flawed authenticator text and damage. The scalability of the software module by changing the parameters of the Niederreiter and/or McEliece MNCCD, depending on the requirements imposed on the communication channels of CRES, ensures its software implementation in mobile gadgets and compatibility with the protocols used for data transmission over the Internet and mobile networks.

The results obtained from the analysis of the threat accumulation are transferred to the 3rd level of the model of strategic management of the bank for their generalization in assessing the adequacy of IR protection technical means in CRES.

Each mechanism for IR protection in CRES $SZ_i \in \{SZ^{KRES}\}$ is characterized by a vector, where T_{SZ} – type of protection, T_V – implementation time, C_{SZ} – cost. Thus, this allows one to study the possibility of «overlapping» with the technical means available in the CISS to provide «confrontation» with modern threats.

The analysis of methods and mechanisms of security in the conditions of hybridity and synergism of modern threats [2, 15, 16, 21, 25–36] demonstrated that cryptographic algorithms are used to provide basic security services (confidentiality, integrity, authenticity). However, in today's development of computing technology, it is advisable to use integrated mechanisms that allow to provide several

Stage 2. Determination of relationships between the CRES infrastructure elements, information assets, threats to the IS, CS, SI and IPH on the basis of the improved model of the CRES infrastructure, synergistic model of threats, advanced threat classifier and attacker mode.

Step 2. 1. Determination of the relationship between IR information assets $\{I_A\}$ and CRES infrastructure elements: $A^{KRES} = \left\| a_{ij}^{KRES} \right\|$.

Step 2. 2. Determination of the relationship between information assets $\{I_A\}$ and objects of the environment: $IO^R = \left\| IO_{il}^R \right\|$, where IO_{il}^R – reflects the presence and type of connection between the i-th information asset and the l-th object of the CRES environment.

Step 2. 3. Determination of the integration of the set of threats. In order to obtain the synergistic effect of increasing the level of protection of IR, consideration should be given to the integration of threats: $DF^{KRES} = \{V^{NS}\} \cup \{V^{AS}\}$, where $\{V^{AS}\} = \{V^{ASBI}\} \cap \{V^{ASIB}\} \cap \{V^{ASKB}\}$.

Step 2. 4. Determination of the cost of the full risk of all assets of the CRES IR. The cost of the full risk equals to the sum of the risk of all assets: $R_{повн} = \sum_{j=1}^{n} R_j$

Step 2. 5. Determination of the probability of implementing at least one threat for each asset of the CRES IR: $p_{rj} = 1 - \prod_{i=1}^{m}\left(1 - pr_{ij}\right)$

Step 2. 6. Determination of the relationship between sources of threats and CRES elements: $A^{DF} = \left\| a_{ij}^{DF} \right\|$.

Fig. 5. Stage 2. Determination of dependencies between elements of the infrastructure of CRES, information assets, threats to the IS, CS, SI and IPH

Stage 3. Determination of the generalized indicator of the level of protection of IR in CRES based on the improved model

Step 3. 1. Determination of the link between threats and IPH:

$$A^{DFSZ} = \left\| a_{ij}^{DFSZ} \right\|, \text{ with } \forall j \in \{I_A\}, \text{ a } \forall i \in \{DF_i\}.$$

$$\left\| A^{DF} \right\| = \begin{cases} 1, \text{if there are } i \text{ threats to } j\text{-th information resource,} \\ 0, \text{if there are no } i \text{ threats to the } j\text{-th information resource.} \end{cases}$$

Step 3. 2. Determination of the set of requirements of regulators $\{RR^{KRES}\}$

$$\{RR^{KRES}\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}$$

Step 3. 3. Determination of the generalized index of the level of protection of CRES, which allows to assess the level of compliance of IPH with the requirements of the regulator:

$OPZ^{KRES} = \sum_{i=1}^{k} OPZ_i$, where k – the number of individual security indicators.

Based on the obtained data, the system is assigned one of three levels of security $UZ^{KRES} = \{\text{low, middle, high}\}$ in accordance to the rule: $UZ^{KRES} = \begin{cases} \text{high, if } OPZ^{KRES} = 3; \\ \text{middle, if } 1 \le OPZ^{KRES} \le 3; \\ \text{low, if } OPZ^{KRES} = 0. \end{cases}$

Fig. 6. Stage 3. Determination of the generalized index of the level of protection of IR in CRES on the basis of the improved model

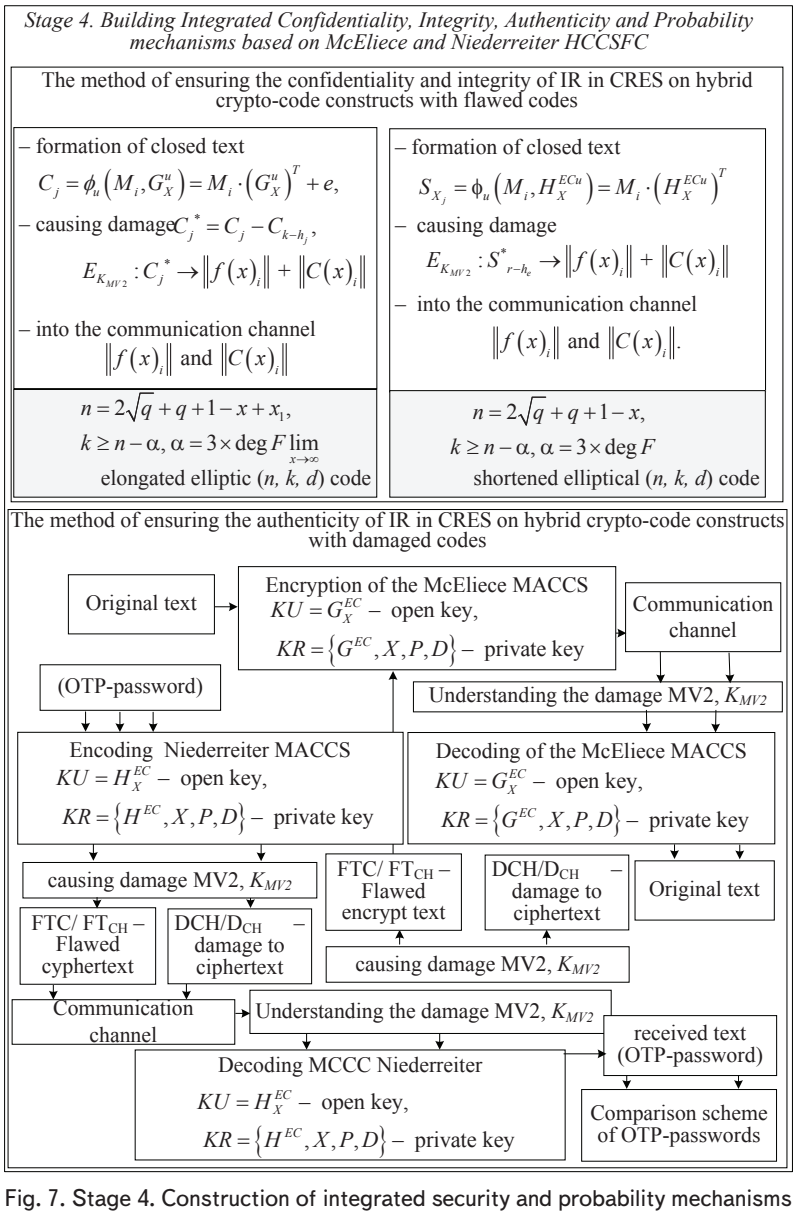

Fig. 7. Stage 4. Construction of integrated security and probability mechanisms

This approach allows us to provide scalability of CRES infrastructure elements, to use new software applications to improve the provision of educational services in the context of the autonomy of the IHE.

7. Conducting an experiment based on the proposed methodology

To evaluate the proposed solutions of methodological principles for building the security system of IP in CRES, we will conduct an experiment.

The source data is *Type* – the type of information asset, described by a set of basic values:

$$Type = \{SD, PID, RrD, ST, StO, Ol, YI, PD\},$$

where *SD* – scientific data; *PID* – payment documents; *KrD* – credit documents; *ST* – research secret; *StO* – statistical reports; *Ol* – public information; *YI* - guiding information; *PD* – personal data. A^K – confidentiality; A^C – integrity; A^D – availability; A^A – Authenticity; C_Y – continuity – the properties of information that need to be provided.

On the basis of the proposed classifier in [17], we determine the possible threats to CRES, which are shown in Table 1.

Taking into account the synergism and hybridity of modern threats, Table 2 presents the results of evaluation of these properties.

The presented results testify to the possibility of CRES cracking in the conditions of application of hybrid threats.

Table 3 shows what services should be provided with protection mechanisms, and Table 4 – the relationship of information assets with elements of the generalized infrastructure of CRES.

Table 1

List of threats to CRES

Threat ID	Content
04.02.03.01	The threat of physical aging of hardware components
03.02.04.04	The threat of failure of the temperature control subsystem
04.04.04.04	The threat of unauthorized use of system and network utilities
02.04.01.03	The threat of software replacement
04.02.03.01	The threat of spreading «post worms»
04.01.02.02	The threat of media formatting
04.01.02.02	The threat of overcoming physical protection
03.01.04.05	The threat of substituting the subject of network access
03.01.04.05	The threat of substituting a trusted user
03.01.04.01	The threat of substituting a wireless client or access point
02.02.03.03	The threat of damage to the system registry
02.03.02.03	The threat of rebooting the hardware and software of the computer
02.03.02.05	The threat of incorrect use of the software functionality
03.01.03.02	The threat of access to local server files using URL
03.02.04.03	The threat of impact on programs with high privileges

Table 2

Results of threat synergy and hybrid assessment

Security components	Security services				
	C, W^{C}_{synerg}	I, W^{1}_{synerg}	A, W_{synerg}	Au, W^{u}_{synerg}	Result
$IS,\ W^{IS}_{synerg}$	0.011	0.064	0.018	0.106	0.0000013
$CS,\ W^{CS}_{synerg}$	0.025	0.056	0.036	0.018	0.0000009
$SI,\ W^{SI}_{synerg}$	0.029	0.019	0.049	0.034	0.0000009
Result	0.065	0.139	0.103	0.158	
$W^{IS,CS,SI}_{synerg} = 0.000003$			$W^{hybrid\ C,I,A,Au}_{synerg} = 0.000147$		

Table 3

Security services of CRES IR

Name, I_{A_i}	*C*	*I*	*A*	*Au*
SD	1	1	1	1
PID	1	1	1	1
KrD	1	1	1	1
ST	1	1	1	1
StO	0	1	1	1
Ol	0	1	1	0
YI	0	1	1	1
PD	1	1	1	1

Table 4

Relationship of information assets with elements of the generalized infrastructure of CRES

Name, I_{A_i}	Physical level	Network level	OS level	DBMS level	AP level
SD	*pt*	*pt*	*so*	*cs*	*so*
PID	*pt*	*pt*	*so*	*cs*	*so*
KrD	*pt*	*pt*	*so*	*cs*	*so*
ST	*pt*	*pt*	*so*	*cs*	*so*
StO	*pt*	*pt*	*so*	*cs*	*so*
Ol	*pt*	*pt*	*so*	*cs*	*so*
YI	*pt*	*pt*	*so*	*cs*	*so*
PD	*pt*	*pt*	*so*	*cs*	*so*

Note: 0 – no relationship, cs – includes and saves, pt – processes or transmits, so – supports operation

In this way, the relationship between the IR of CRES, CRES infrastructure elements, communication lines and IR security services is ensured.

Tables 5, 6 present the results of investigations of interrelations between threats and the CRES IR (Table 5), and the threats and CRES infrastructure elements (Table 6). This allows you to determine the critical points (Table 6 – probability is equal to one) in the protection system, and the probability of unauthorized access to the corresponding asset of CRES IR.

Table 5

Determining the probability of implementing at least one threat for each IR asset

Threat ID	*SD*	*PID*	*KrD*	*ST*	*StO*	*Ol*	*YI*	*PD*
04.02.03.01	0.268	0.268	0.268	0.268	0.241	0.222	0.241	0.268
03.02.04.04	0.267	0.267	0.267	0.267	0.179	0.091	0.179	0.267
04.04.04.04	0.068	0.068	0.068	0.068	0.063	0.029	0.063	0.068
02.04.01.03	0.2	0.2	0.2	0.2	0.182	0.132	0.182	0.2
04.02.03.01	0.268	0.268	0.268	0.268	0.241	0.222	0.41	0.268
04.01.02.02	0.067	0.067	0.067	0.067	0.05	0.044	0.05	0.067
04.01.02.02	0.067	0.067	0.067	0.067	0.05	0.044	0.05	0.067
03.01.04.05	0.088	0.088	0.088	0.088	0.088	0	0.088	0.088
03.01.04.05	0.088	0.088	0.088	0.088	0.088	0	0.088	0.088
03.01.04.01	0.088	0.088	0.088	0.088	0.088	0	0.088	0.088
02.02.03.03	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
02.03.02.03	0.2	0.2	0.2	0.2	0.166	0.1	0.166	0.2
02.03.02.05	0.333	0.333	0.333	0.333	0.226	0.143	0.226	0.333
03.01.03.02	0.267	0.267	0.267	0.267	0.267	0	0.267	0.267
03.02.04.03	0.133	0.133	0.133	0.133	0.1	0.056	0.1	0.133

Table 6

Determining the relationship between sources of threats and CRES elements

Threat ID	Physical level	Network level	OS level	DBMS level	AP level
04.02.03.01	0.44968	0.44968	0.34748	1	0.34748
03.02.04.04	0.39248	0.39248	0.30328	0.892	0.30328
04.04.04.04	0.1089	0.1089	0.08415	0.2475	0.08415
02.04.01.03	0.32912	0.32912	0.25432	0.748	0.25432
04.02.03.01	0.44968	0.44968	0.34748	1	0.34748
04.01.02.02	0.231	0.231	0.1785	0.525	0.1785
04.01.02.02	0.231	0.231	0.1785	0.525	0.1785
03.01.04.05	0.06776	0.06776	0.05236	0.154	0.05236
03.01.04.05	0.13552	0.13552	0.10472	0.308	0.10472
03.01.04.01	0.13552	0.13552	0.10472	0.308	0.10472
02.02.03.03	0.176	0.176	0.136	0.4	0.136
02.03.02.03	0.31504	0.31504	0.24344	0.716	0.24344
02.03.02.05	0.4972	0.4972	0.3842	1	0.3842
03.01.03.02	0.41118	0.41118	0.31773	0.9345	0.31773
03.02.04.03	0.20262	0.20262	0.15657	0.4605	0.15657

Table 7 gives the result of studying the ability of information security systems to resist threats.

Table 7

Relationship between threats and TTIP

Threat ID	Physical level	Network level	OS level	DBMS level	AP level
04.02.03.01	MZ	MZ	MZ	MZ	MZ
03.02.04.04	MZ	MZ	MZ	MZ	MZ
04.04.04.04	MZ	MZ	MZ	MZ	MZ
02.04.01.03	MZ	MZ	MZ	MZ	MZ
04.02.03.01	MZ	MZ	MZ	MZ	MZ
04.01.02.02	MZ	MZ	MZ	MZ	MZ
04.01.02.02	MZ	MZ	MZ	MZ	MZ
03.01.04.05	MZ	MZ	MZ	MZ	MZ
03.01.04.05	MZ	MZ	MZ	MZ	MZ
03.01.04.01	MZ	MZ	MZ	MZ	MZ
02.02.03.03	MZ	MZ	MZ	MZ	MZ
02.03.02.03	MZ	MZ	MZ	MZ	MZ
02.03.02.05	MZ	MZ	MZ	MZ	MZ
03.01.03.02	MZ	MZ	MZ	MZ	MZ
03.02.04.03	MZ	MZ	MZ	MZ	MZ

The model uses the following types of communication: MZ – there is a protection mechanism that provides counteraction to its destructive effect; NMZ – there is no protection mechanism against the i-th threat.

On the basis of the conducted research and assessment of the implementation of the requirements of regulators, we will define a generalized indicator of the level of protection of IR in CRES, which allows us to assess the level of compliance of IPH with the requirements of regulators and is determined by:

$$OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i,$$

where k – the number of individual security indicators, OPZ_i – a separate indicator that takes the value of the set: OPZ_1 – the absence of unacceptable risks, if during drawing up a threat model/intruder model and risk assessment unacceptable threats are revealed in an IHE, then $OPZ_1=0$, otherwise – $OPZ_1=1$; OPZ_2 – absence of dangerous threats unclosed by TTIP mechanisms, $OPZ_2=0$, in the case when during the compilation of the model «uncovered» threats are revealed in the IHE – $OPZ_2=1$; OPZ_3 – level of IR security compliance with regulatory requirements recognized as recommended – $OPZ_3=1$, if not recognized as recommended – $OPZ_3=0$.

In order to ensure the quality of investment in the IS system, it is proposed to use an improved method based on the results of the generalized OPZ^{KRES} security level indicator, a generalized synergistic threat $W_{synerg}^{IS,CS,SI}$, of a set of assets $\{I_A\}$, a set of elements of the information assets of CRES. The proposed investment estimation model [3] is determined by the state of the model of investment efficiency in the CRES IR IS on the following steps.

Step 1. Estimating the level of return on investment in IS:

$$ROI^{KRES} = NPV_{inv}^{KRES} - NPV_{zt}^{KRES},$$

where NPV_{inv}^{KRES} – return on investment in IPH (ISS) of CRES; NPV_{zt}^{KRES} – costs in TMIP (ISS) of CRES; ROI^{KRES} – return on investment in (ISS) of CRES.

Step 2. Estimation of the ROI in IPH:

$$ROSI^{KRES} = NPV_{IPH}^{KRES} - NPV_{IPH}^{KRES},$$

where NPV_{IPH}^{KRES} – costs of eliminating the security compromise without the implementation of IPH (ISS); NPV_{IPH}^{KRES} – costs of eliminating the security compromise with the implementation of IPH (ISS).

Step 3. Estimation of net present value:

$$NPV_{IPH}^{KRES} = \sum_{i=1}^{N} \frac{ALE_i}{(1+r)^i}, \quad NPV_{IPH}^{KRES} = C_{sz} + \sum_{i=1}^{N} \frac{ALE_i}{(1+r)^i},$$

where N – the number of investment intervals, ALE_i – the expected cost in the i-th period, r – discount rate, C_{sz} – cost of remedies.

Step 4. Risk estimation of IR by the calculation method *Annual loss expectancy – ALE*, i. e. expected losses in each period of evaluation –

$$ALE^{KRES} = \sum_{i=1}^{n} I\left(O_{DF}^{ABS}\right) F_i,$$

where $\{O_{DF}^{KRES}\}$ – the set of threats; $I(O_{DF}^{KRES})$ – the cost implications of the threat; ALE^{KRES} – expected loss from implementation; F_i – frequency (possibility) of implementation of the threat.

Step 5. Estimation of potential losses U^{KRES} of the information asset – $U^{KRES}=p_{rj}u_j$, where p_{rj} – probability of implementation of at least one threat of the j-th asset; u_j – the value of the j-th asset.

Step 6. Estimation of the total expected loss:

$$OU^{KRES} = \sum_{j=1}^{n} U^{KRES}.$$

Summarizing the parameters used in the proposed model, we will define the integral efficiency criterion of the investment in the security of the IR of CRES, using the expression:

$$W_{KRES}^{effinv} = \sum_{i=1}^{N} w_i M^{KRES}.$$

Thus, the efficiency model of investment in the security of the IR of CRES can be in different states S^{KRES}, that can be described as the following set:

$$S^{KRES} = \{S_1^{KRES}, S_2^{KRES}, ..., S_m^{KRES}\},$$

where S^{KRES} – the set of possible states of the model; S_1^{KRES} – the initial state of the model; S_m^{KRES} – the final state of the model.

In the calculations, assume that the provision of IS in IHE, a university spends up to 4 % of the annual budget, the cost of developing IPH is up to 2 % of the annual budget, the probable costs of eliminating the security compromise without implementation up to 5 % of the annual budget, the probable costs of eliminating the security compromise up to 2 % of the annual profit, C_{sz} – the cost of protection means is 30 % of the total cost of IR. The discount rate is 13 %. The results of the overall efficiency indicator are shown in Table 8.

Table 8

Results of the total expected loss, consequences of decommissioning of IPH, thousand c. u.

Name, I_{A_i}	W_{KRES}^{effinv} for the components of security services				Total
	C	*I*	*A*	*Au*	
SD	0.0391	0.0294	0.0196	0.0098	0.09792
PID	0.0098	0.0073	0.0049	0.0024	0.02448
KrD	0.0588	0.0441	0.0294	0.0147	0.14688
ST	0.0392	0.0294	0.0196	0.0098	0.09792
StO	0.0059	0.00441	0.0029	0.0015	0.01469
Ol	0.0039	0.0029	0.0020	0.0010	0.00979
YI	0.0196	0.0147	0.0098	0.0049	0.04896
PD	0.0196	0.01467	0.0098	0.0049	0.04896
$W_{KRES_{general\,1_{A_i}}}^{effinv}$	0.1958	0.14688	0.09792	0.04896	
$W_{KRES_{general}}^{effinv} = W_{KRES_{general\,1_{A_i}}}^{effinv\ \ C} \cap W_{KRES_{general\,1_{A_i}}}^{effinv\ \ I} \cap W_{KRES_{general\,1_{A_i}}}^{effinv\ \ A} \cap W_{KRES_{general\,1_{A_i}}}^{effinv\ \ Au} =$ $= 0.0001379$					

8. Discussion of the results of the proposed methodology

The concept of constructing a synergistic model of threats to the security of information resources of CRES, which is based on the three-level model of strategic security management of information technology of CRES, is proposed. The concept covers all the main areas of development of the IHE on the security of information resources, based on a synergistic approach to the selection of the most effective directions for achieving the goals of security of information resources at each level of the management model in the conditions of autonomy of higher education institution.

The proposed classifier of threats to the security of information resources, unlike existing ones, is based on a synergistic model of threats that allows to classify threats by security components, service types and hierarchy levels of the CRES infrastructure, to assess the synergy and hybridity of threats to information security, cyber security, security of information, probability of their impact on the security of information resources. The proposed classifier is universal and can be used in assessing the threats of any CCIS. Practical implementation of the classifier will allow in online mode to form expert assessment of the level of threats to information resources, analyze their synergy and hybridity, assess the probability of the impact of threats to information security, cybersecurity, security of information on the security of information resources without significant investment and human resources.

The proposed method for evaluating the generalized indicator of the level of protection of information resources of CRES and the practical methodology for assessing the level of protection of information resources of CRES based on a synergistic model of threats, advanced threat classifier and attacker model, model for assessing the security of information resources and model of the CRES infrastructure allow to optimize the cost of building a security system of information resources of IHE. Practical significance is the ability to timely assess the interconnections between assets of information resources, infrastructure elements, technical means of protection in CRES and possible manifestations of threats to information security, cyber security and security of information. This allows you to timely correct the IHE management documents on information security, plan investment in the technical means of information protection, to formulate preventive measures to prevent threats.

The method of ensuring the confidentiality and integrity of information resources on hybrid crypto-code systems with flawed codes is proposed. The method is based on the modified McEliece crypto-code system on modified algebra-geometric codes, which allows integrated (with one mechanism) provision of the security of information resources (safe time – $T_{security} > 200$, resistance to cryptanalysis of $P_{cryptanalysis} < 10^{25}–10^{35}$ group operations), transmission reliability of information resources in CRES ($P_{error} < 10^{-9}$) and reduction of energy costs for their practical implementation 10^{-12} times (encryption, decryption) by reducing the order of $GF(q)$.

For the experimental study of the proposed modified asymmetric crypto-code systems (MACCS) on modified elliptic codes (MEC), hybrid crypto-code systems on flawed codes (HCCSFC), the corresponding software mock-ups were implemented. The results of comparative studies of McEliece ACCS, McEliece MACCS on *MEC*, and HCCSFC are given in Tables 9, 10.

Table 9

Results of analysis of hacking complexity and coding complexity for different speeds of *EC* (*MEC*)

$lg(l_s)$	Relative encoding speed, *R*					
	0.5	0.75	0.5(*ud*)	0.75(*ud*)	0.5(*uk*)	0.75(*uk*)
1	4.75	12.1	15.6	18.23	19.12	19.82
2	10.52	21.76	32.47	35.67	38.63	39.18
3	18.22	33.17	43.75	51.61	56.88	58.03
4	21.42	51.75	59.43	72.81	78.92	80.52
5	38.77	61.09	68.26	87.32	94.91	104.56
6	54.13	78.37	**101.72**	**112.46**	**120.83**	**128.79**
7	82.14	83.72	156.75	164.72	182.39	189.74
8	165.84	179.13	223.64	231.57	276.27	287.33
9	358.33	371.09	421.97	428.63	459.81	476.52
10	**672.37**	**684.94**	716.41	722.26	783.46	794.28

Table 10

Results of analysis of hacking complexity and coding complexity for different speeds *MEC* (*MEC+FLAWED CODES*)

$lg(l_s)$	Relative encoding speed, *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

In Tables 9, 10, conditional abbreviations (prefixes) were used: *ukh/udh* – hybrid CCSFC with shortened *MEC*/hybrid CCSFC with elongated *MEC*; *uk* – MACCS with shortened *MEC*; *ud* – MACCS with elongated *MEC*. In the calculations of the parameters of the cryptosystems, Galois fields were used: for McEliece ACCS – $GF(2^{10})$; for MACCS with shortened/lengthened *MEC* – $GF(2^6)$; for hybrid CCSFC – $GF(2^4)$.

McEliece ACCS *on elliptic codes (EC)*:

The complexity of the decoding process for ATCS on EC is given by the expressions:

– for ATCS on *EC*: $O_{K+}=N_{coverings}\cdot n\cdot r$, where

$$N_{coverings}\geq\frac{C_n^{\rho\cdot t}}{C_{n-k}^{\rho\cdot t}}=\frac{n(n-1)...(n-\rho\cdot t-1)}{(n-k)(n-k-1)...(n-k-\rho\cdot t-1)},$$

$$t=\lfloor(d-1)/2\rfloor,$$

– for MACCS on shortened codes:

$$O_{K+}=N_{coverings}\times\left(2\sqrt{q}+q+1-1/2k\right)\times r;$$

– for MACCS on elongated codes:

$$O_{K+}=N_{coverings}\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)\times r.$$

The complexity of the decoding process for HCCSFC on shortened MEC has the form:

– for HCCSFC on shortened *MEC*:

$$O_{K+}=N_{coverings}\times\left(2\sqrt{q}+q+1-1/2k\right)\times r+N_F \text{ or } (N_K),$$

where

$$N_F\approx\frac{K_C{}^z}{2^{1-K_C{}^{z+1}}}\times|F|;\ K_C=97/128;$$

$|F|$ – total length of output banners (flaws) (bits) – with a remnant known to the attacker (flawed text) and specified banners (flaws), with an unknown key: $N_K\approx 2^{1190\times z}$; $z=16$;

– for HCCSFC on elongated *MEC*:

$$O_{K+}=N_{coverings}\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)\times r+N_F \text{ or } (N_K).$$

Analysis of Tables 9, 10 confirms that the use of flawed codes and the subsequent reduction of the power of the Galois field lead to a significant reduction in the complexity of formation (≈12 times) and decoding of the cryptogram (≈20 times).

Tables 11, 12 show the results of investigations of the dependence of capacitive characteristics on the Galois field power for software implementation.

Implementation of the proposed method allows to increase the level of protection of information resources and to ensure timely response to the requirements of international and national security regulators of information resources through the modification of certain parameters and modification of the use of modified McEliece and Niederreiter crypto-code systems with multichannel cryptography systems on flawed codes.

The proposed method of two-factor authentication on hybrid crypto-code systems with flawed codes based on modified McEliece and Niederreiter crypto-code systems with *MEC* allows to ensure the level of stability of *OTP* passwords in the transmission over open communication channels and to preserve the possibility of further use of the two-factor authentication protocol based on *SMS* messages. In spite of decreasing the Galois field power to $GF(2^6)$ for modified crypto-code systems and $GF(2^4)$ for hybrid crypto-code systems on flawed codes, the statistical characteristics of such crypto-code systems were at least not worse than the traditional McEliece systems over $GF(2^{10})$.

Table 13 presents the results of studies of statistical properties of the proposed methods based on the *NIST STS* 822 package.

Table 13 demonstrated that, despite the decrease of the Galois field power to $GF(2^6)$ for MACCS and $GF(2^4)$ for HCCSFC, the statistical characteristics of such crypto-code structures were at least not worse than the traditional McEliece ACCS on $GF(2^{10})$. All cryptosystems passed 100 % tests, with the best result revealed by the HCCSFC on shortened *MEC:* 155 out of 189 tests passed at the level of 0.99, which is 82 % of the total number of tests. In this case, the traditional McEliece ACCS on $GF(2^{10})$ showed 149 tests at 0.99. In this way, the proposed methods provide basic security services and the required level of sustainability and reliability of IRS.

Table 11

Dependence of software implementation speed on the field power (number of group operations)

Cryptosystems	$GF(q^m)$					
	2^5	2^6	2^7	2^8	2^9	2^{10}
McEliece ACCS on *EC*	10018042	18048068	32847145	47489784	63215578	82467897
McEliece MACCS on shortened *MEC*	10007947	**17787431**	28595014	44079433	61974253	79554764
McEliece MACCS on elongated *MEC*	11156138	**18561228**	33210708	48297112	65171690	84051337

Table 12

Dependence of software implementation speed on the field power (number of group operations)

Cryptosystems	$GF(q^m)$						
	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
McEliece MACCS on shortened *MEC*	8293075	10007947	**17787431**	28595014	44079433	61974253	79554764
McEliece MACCS on elongated *MEC*	8506422	11156138	**18561228**	33210708	48297112	65171690	84051337
HCCSFC on elongated *MEC*	**5612316**	7900315	14892945	25565274	42279183	58963778	76564173
HCCSFC on shortened *MEC*	**5942627**	7905257	14682411	25595014	42116327	58468143	75474764

Table 13

Results of statistical safety research

Cryptosystems	The number of tests of more than 99 % of the sequences	The number of tests of more than 96 % of the sequences	The number of tests of less than 96 % of the sequences
McEliece ACCS on *EC*	149 (78.83 %)	189 (100 %)	0 (0 %)
McEliece MACCS on shortened *MEC*	151 (79.89 %)	189 (100 %)	0 (0 %)
McEliece MACCS on elongated *MEC*	152 (80.42 %)	189 (100 %)	0 (0 %)
HCCSFC on elongated *MEC*	**153 (80.95 %)**	189 (100 %)	0 (0 %)
HCCSFC on shortened *MEC*	**155 (82 %)**	189 (100 %)	0 (0 %)

The proposed method for assessing the safety of information resources, which, unlike the known, takes into account the integrated indicator of the efficiency of investments, which are allocated to ensure the security of information resources, allows you to optimize the cost of its construction under the influence of hybrid threats, while providing a certain level of their security. Practical implementation of the method allows to comprehensively assess the main indicators of investment in ensuring the security of information resources, taking into account synergistic assessment of threats to information security, cybersecurity and security of information.

The promising direction of research is the practical implementation of the proposed solutions in the IHE CRES.

9. Conclusions

1. Analysis of the organization of autonomy demonstrates that it is necessary to use a modern corporate network that should provide the required level of quality of service in order to perform the functions of institutional autonomy. Such system refers to critical cybernetic information systems. There are current hybrid threats with signs of synergy that affect the elements of the CRES infrastructure and they require appropriate destructive counteraction measures. At the same time, at present, there are no relevant legislative acts that would contribute to the construction of a comprehensive system for the protection of information resources of CRES. Therefore, there is a need to formulate a methodology for building a system of information security in the corporate scientific and educational system under the conditions of university autonomy.

2. The concept of building a synergistic model of threats to the security of information resources of CRES, which is based on a three-level model of strategic management of information technology security, is proposed. The model developed on the basis of the concept through the integration of the components of information security, cyber security and security of information opens a new direction in ensuring the security of information resources. The proposed approach based on the model of institutional autonomy management taking into account the magnitude of risk at each level and effective control over the implementation of the functions of the information security management system of higher education institutions allows to provide a certain level of security of the CRES IR.

3. The proposed methodology for building an information security system in CRES, in contrast to well-known approaches, implements a fundamentally new concept of countering hybrid threats to the education sector. Its essence and content consist in rational organization of the system of maintenance of IR IS in CRES under the conditions of simultaneous action of threats to information security, cybersecurity and security of information on the system. This approach allows for a complete and adequate assessment of the IR level in CRES, which significantly influences the value of security investments in the education sector in terms of autonomy and opens the way for management decisions making on security issues.

The methodology is based on the proposed three-level model of strategic management of information technology security in the IHE. On the basis of the developed methodology, the classifier of threats to information security has become further developed in terms of simultaneous consideration of, in addition to threats to information security, threats to cybersecurity and threats to the security of information of IR in CRES. The introduction of the classifier allowed us to conclude that it would be advisable to use the integrated mechanisms for providing services based on the HCCSFC to counter the hybrid threats to IR in CRES.

References

1. Androshchuk H. O. Kiberbezpeka: tendentsiyi v sviti ta Ukraini // Kiberbezpeka ta intelektualna vlasnist: problemy pravovoho zabezpechennia: materialy Mizhnarodnoi naukovo-praktychnoi konferentsiyi. Kyiv: Vyd-vo «Politekhnika», 2017. P. 30–36.
2. Grischuk R. V., Danik Yu. G. Osnovy kiberbezopasnosti: monografiya / Yu. G. Danik (Ed.). Zihtomir: ZHNAEU, 2016. 636 p.
3. Assessment of functional efficiency of a corporate scientific-educational network based on the comprehensive indicators of quality of service / Yevseiev S., Ponomarenko V., Ponomarenko V., Rayevnyeva O., Rayevnyeva O. // Eastern-European Journal of Enterprise Technologies. 2017. Vol. 6, Issue 2 (90). P. 4–15. doi: https://doi.org/10.15587/1729-4061.2017.118329
4. Hryshchuk R. V., Korchenko O. H. Metodolohiya syntezu ta analizu dyferentsialno-ihrovykh modelei ta metodiv modeliuvannia protsesiv kibernapadu na derzhavni informatsiyni resursy // Ukrainian Information Security Research Journal. 2012. Vol. 14, Issue 3. P. 115–122. doi: https://doi.org/10.18372/2410-7840.14.3418

5. Baranov H., Zakharova M., Hornitska D. Methodology for the synthesis of systems security level evaluation of public information resources from social engineering attacks // Ukrainian Information Security Research Journal. 2012. Vol. 14, Issue 3. P. 98–104. doi: https://doi.org/10.18372/2410-7840.14.3396
6. Synthesis methodology and software implementation system evaluation harm to national security in protection of state secrets / Korchenko A., Luttskyy M., Zaharova M., Dreys Y. // Ukrainian Information Security Research Journal. 2013. Vol. 15, Issue 1. P. 14–20. doi: https://doi.org/10.18372/2410-7840.15.4210
7. Rajba S., Karpinski M., Korchenko O. Generalized models, construction methodology and the application of secure wireless sensor networks with random network parameters // Ukrainian Scientific Journal of Information Security. 2014. Vol. 20, Issue 2. P. 120–125. doi: https://doi.org/10.18372/2225-5036.20.7296
8. Yudin A., Buchyk S. Methodology of defence of state informative resources. Comparative analysis of basic terms and determinations // Ukrainian Information Security Research Journal. 2015. Vol. 17, Issue 3. P. 218–225. doi: https://doi.org/10.18372/2410-7840.17.9518
9. Zhurilenko B. Construction and analysis methodology of complex technical information security with probabilistic reliability and counting of temporal breaking attempts // Ukrainian Information Security Research Journal. 2015. Vol. 17, Issue 3. P. 196–204. doi: https://doi.org/10.18372/2410-7840.17.9515
10. Buchyk S. The methodology of analysis of risks of tree that identifiers the state informative resources // Ukrainian Information Security Research Journal. 2016. Vol. 18, Issue 1. P. 81–89. doi: https://doi.org/10.18372/2410-7840.18.10116
11. Korchenko A., Shcherbyna V., Vyshnevska N. A methodology for building cyberattack-generated anomaly detection systems // Ukrainian Information Security Research Journal. 2016. Vol. 18, Issue 1. P. 30–38. doi: https://doi.org/10.18372/2410-7840.18.10110
12. Ivanchenko E., Kazmirchuk S., Gololobov A. Metodologiya sinteza sistem analiza i otsenki riskov poter' informatsionnyh resursov // Ukrainian Information Security Research Journal. 2012. Vol. 14, Issue 2. P. 5–9. doi: https://doi.org/10.18372/2410-7840.14.2178
13. Shiyan A. Methodology of complex security for the person and social groups against the negative information-psychological influence // Ukrainian Scientific Journal of Information Security. 2016. Vol. 22, Issue 1. P. 94–98. doi: https://doi.org/10.18372/2225-5036.22.10460
14. Korchenko O., Kazmirchuk S., Ivanchenko E. The methodology for the synthesis of adaptive risk assessment systems of security information system resources // Ukrainian Information Security Research Journal. 2017. Vol. 19, Issue 3. P. 198–204. doi: https://doi.org/10.18372/2410-7840.19.11898
15. Boyarov E. N. Klyuchevye problemy informatsionnoy bezopasnosti sfery obrazovaniya // Pedagogika vysshey shkoly. 2016. Issue 3.1. P. 42–45. URL: https://moluch.ru/th/3/archive/43/1500/
16. Dorozhkin A. V., Yasenev V. N., Yasenev O. V. Metodologicheskie aspekty obespecheniya informatsionnoy bezopasnosti v VUZe // Innovatsionnye metody obucheniya v vysshey shkole. 2016. P. 77–83.
17. 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. doi: https://doi.org/10.29013/r.hryshchuk_s.yevseiev_a.shmatko.cmissbiabs.284.2018
18. Ansari M. T. J., Pandey D., Alenezi M. STORE: Security Threat Oriented Requirements Engineering Methodology // Journal of King Saud University - Computer and Information Sciences. 2018. doi: https://doi.org/10.1016/j.jksuci.2018.12.005
19. Timpson D., Moradian E. A Methodology to Enhance Industrial Control System Security // Procedia Computer Science. 2018. Vol. 126. P. 2117–2126. doi: https://doi.org/10.1016/j.procs.2018.07.240
20. A Bayesian network methodology for optimal security management of critical infrastructures / Misuri A., Khakzad N., Reniers G., Cozzani V. // Reliability Engineering & System Safety. 2018. doi: https://doi.org/10.1016/j.ress.2018.03.028
21. Machine-Learning-Based Side-Channel Evaluation of Elliptic-Curve Cryptographic FPGA Processor / Mukhtar N., Mehrabi M., Kong Y., Anjum A. // Applied Sciences. 2018. Vol. 9, Issue 1. P. 64. doi: https://doi.org/10.3390/app9010064
22. Rehman S., Gruhn V. An Effective Security Requirements Engineering Framework for Cyber-Physical Systems // Technologies. 2018. Vol. 6, Issue 3. P. 65. doi: https://doi.org/10.3390/technologies6030065
23. Bodei C., Chessa S., Galletta L. Measuring security in IoT communications // Theoretical Computer Science. 2019. Vol. 764. P. 100–124. doi: https://doi.org/10.1016/j.tcs.2018.12.002
24. Hudic A., Smith P., Weippl E. R. Security assurance assessment methodology for hybrid clouds // Computers & Security. 2017. Vol. 70. P. 723–743. doi: https://doi.org/10.1016/j.cose.2017.03.009
25. Alguliyev R., Imamverdiyev Y., Sukhostat L. Cyber-physical systems and their security issues // Computers in Industry. 2018. Vol. 100. P. 212–223. doi: https://doi.org/10.1016/j.compind.2018.04.017
26. Rezgui Y., Marks A. Information security awareness in higher education: An exploratory study // Computers & Security. 2008. Vol. 27, Issue 7-8. P. 241–253. doi: https://doi.org/10.1016/j.cose.2008.07.008
27. Schneider F. B. Cybersecurity Education in Universities // IEEE Security & Privacy. 2013. Vol. 11, Issue 4. P. 3–4. doi: https://doi.org/10.1109/msp.2013.84

28. Conklin A. Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course // Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06). 2006. doi: https://doi.org/10.1109/hicss.2006.110
29. Method and Model of Analysis of Possible Threats in User Authentication in Electronic Information Educational Environment of the University / Lakhno V. A., Kasatkin D. Y., Blozva A. I., Gusev B. S. // Advances in Computer Science for Engineering and Education II. 2020. P. 600–609. doi: https://doi.org/10.1007/978-3-030-16621-2_56
30. Models and Algorithms of Vector Optimization in Selecting Security Measures for Higher Education Institution's Information Learning Environment / Akhmetov B., Lakhno V., Akhmetov B., Myakuhin Y., Adranova A., Kydyralina L. // Intelligent Systems in Cybernetics and Automation Control Theory. 2019. P. 135–142. doi: https://doi.org/10.1007/978-3-030-00184-1_13
31. Kolgatin A. G. Informatsionnaya bezopasnost' v sistemah otkrytogo obrazovaniya // Obrazovatel'nye tekhnologii i obschestvo. 2014. P. 417–425.
32. Anikin V., Emaletdinova L. Yu., Kirpichnikov A. P. Metody otsenki i upravleniya riskami informatsionnoy bezopasnosti v korporativnyh informatsionnyh setyah // Vestnik Kazanskogo tekhnologicheskogo universiteta. 2015. Vol. 18, Issue 6. P. 195–197.
33. Litvinov V. A., Lypko E. V., Yakovleva A. A. Informatsionnaya bezopasnost' vysshego uchebnogo zavedeniya v ramkah sovremennoy globalizatsii. URL: http://conference.osu.ru/assets/files/conf_reports/conf13/132.doc
34. Vahonin S. Udalennyy dostup i utechka dannyh // Informatsionnaya bezopasnost'. 2014. Issue 5. URL: http://www.itsec.ru/articles2/Inf_security/udalennyy-dostup-i-utechka-dannyh/
35. Zamaraeva O. A., Titov V. A., Kuzin D. O. Development of policy of information security for economic higher education institution: definition of information which is subject to protection, and creation of model of the malefactor // Modern problems of science and education. 2014. Issue 3. URL: https://www.science-education.ru/ru/article/view?id=13106
36. Stepanova I. V., Mohammed Omar A. A. Use of advanced technologies for development distributed corporate communication networks // T-Comm. 2017. Vol. 11, Issue 6. P. 10–15.
37. Practical implementation of the Niederreiter modified cryptocode system on truncated elliptic codes / Yevseiev S., Tsyhanenko O., Ivanchenko S., Aleksiyev V., Verheles D., Volkov S. et. al. // Eastern-European Journal of Enterprise Technologies. 2018. Vol. 6, Issue 4 (96). P. 24–31. doi: https://doi.org/10.15587/1729-4061.2018.150903
38. Yevseiev S. The use of damaged codes in crypto code systems // Systemy obrobky informatsiyi. 2017. Issue 5 (151). P. 109–121. doi: https://doi.org/10.30748/soi.2017.151.15