BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 4, Number 380 (2019), 154 – 169 **https://doi.org/10.32014/2019.2518-1467.104**

L. Kydyralina[1], B. Akhmetov[1], V. Lakhno[2], A. Adranova[1]

[1]Kazakh national pedagogical university named after Abay, Almaty, Kazakhstan,
[2]National university of Life and Environmental Sciences of Ukraine, Ukraine.
E-mail: Lazat_75@mail.ru, bakhytzhan.akhmetov.54@mail.ru, valss21@ukr.net, aselhan.adranova@mail.ru

REVIEW AND ANALYSIS OF PREVIOUS RESEARCHES IN THE SPHERE OF ENSURING THE PROTECTION OF INFORMATION AND EDUCATIONAL ENVIRONMENT OF UNIVERSITIES

Abstract. The paper reviewed and analyzed previous researches in the field of protection of the information and educational environment of universities (IEEU). It is shown that the priority development of digital education systems in many industrialized countries of the world requires appropriate technical and methodological support of specialists not only in the field of pedagogical activity, but also in information technology, taking into account the problems of cyber security and information protection. It is shown that the protected data that is stored and circulate in the information and communication systems of universities, in particular, include: personal data of students, teachers, researchers, support staff; digitized information representing the intellectual property of an educational institution; information arrays that provide educational process (for example, multimedia content, databases, tutorials); others. It is substantiated that these information resources can act as an object of theft or distortion from external (internal) computer intruders or from hooligan motives, from the side of students or employees.

It is substantiated that the trend towards globalization of access to information resources, formed in many countries, makes relevant the task of implementation the latest digital and information and communication technologies in all areas of activity of a modern university. The relevance of research in the direction of development of the models for decision support systems for finding investment control strategies for various ratios of the parameters of the investment process in the cyber security systems of educational institutions is also proved. There is shown the necessity of computer support for solving problems of finding investment control strategies in the cyber security strategies of educational institutions. There is described the necessity of developing a conceptual model of the adaptive control of cyber security of an informatization object on the example of IEEU.

Key words: cybersecurity, information and communication environment, educational institution, game theory, decision-making support, a choice of financial strategy.

1.1. Prerequisites for the formation of a safe information and education a lenvironment of a modern university. The priority of digital education systems development in many industrialized countries of the world required appropriate technical and methodological support of specialists not only in the field of educational activities, but also in the field of IT. Therefore, the trend towards globalization of access to information resources, formed in many countries, makes relevant the task of implementation the latest digital and information and communication technologies in all areas of activity of a modern university [1, 2].

At the end of the last century, but especially active at the beginning of 21st century, there was used the term “information and educational environment of the university” [1]. This concept in many scientific publications [3,4] is interpreted as: "A set of computer tools and methods of their functioning, which are used in order to implement learning activities" [2, 5]. Many aspects of the creation of the IEEU have already been studied in detail in the works of such authors as Mikhnev IP [6], Conklin A.[10], Gordon LA. [15] and others. In Kazakhstan, similar researches were carried out by Bidaybekov EY.[19], Nurgaliyeva KK. [20], Shafeev DE[2], Tleuberdiyeva G. [17], Kubieva TSh. [14] and others. However, beyond the framework of most existing researches on the development of IEE of the universities, there are aspects related to the tasks of ensuring the information protection and cybersecurity of information and

communication systems of the universities from any kind of destructive interference by computer intruders.

The globalization of education brought the questions about the use of information technologies and systems (ITS) in universities to the first place. However, the attention was not always paid to the parallel consideration of the tasks of ensuring information and cybersecurity (hereinafter, respectively, IS and CS) of both staff and students.

IT specialists have repeatedly noted [1,3,6] that in the tasks of IS and CS support the resource provision and protective mechanisms management of the universities (equally to other educational institutions (EI)) requires solving a number of problems:

1) the need to eliminate the lack of equipment with technical means of information protection (TMIP);

2) the lack of specialized training of personnel responsible for IS and CS of the university;

3) optimization in the tasks of the targeted funding distribution for IS and CS of the university;

4) and another.

Modern educational institutions unite beyond their walls a large number of highly qualified teachers, staff of research departments, students, as well as support staff.

However, constantly accumulating a variety of information, both of educational and methodological direction, as well as other data, for example, which connected with the EI, personal data of employees and students, IT specialists of universities faced to additional problems [7]. First of all, we should note the lack of a clear procedure in the accumulation process and in practical application of disparate and diversely formatted information resources. However, these resources often do not undergo an audit procedure regarding their IS and CS. Many of the software products installed in the university's information and educational environment (IEEU) are not related to each other, are often obtained from unreliable or compromised sources, therefore, they may pose a potential danger to IEEU.

To the protected data, stored and circulated in the information and communication systems of universities (ICSU), there can be attributed [2, 4, 7]:

- personal data of students, teachers, researchers, support staff;
- digitized information representing the intellectual property of the educational institution;
- information arrays that provide the learning process (for example, multimedia content, databases, training programs);
- others.

This information can act as an object of theft or distortion from external (internal) computer intruders (CI) or from hooligan motives, from students or employees.

During the dissertation research, there was performed an analysis based on the results of an audit of IS and CS of international companies dealing with relevant issues for state organizations, including universities and other large educational institutions (EI). First of all, they are EU, the USA and Canada [7, 8]. As the results of such studies [4,8] showed, as well as the data cited in [9,10], and not taking into account specific targeted attacks aimed at buffer overflow and violation of cryptographic protocols [11], a significant amount of violations is associated with unauthorized data changes in IEEU (> 12%), with bypassing the restrictions policy on IS in IEEU (> 15%), with insufficient protection of the authentication procedure, etc., see figures 1.1 and 1.2.

Different according to the source data [8,11] can be the targets, objects and subjects of cyber attacks on IEEU, see table 1.1.

Also, in there were noted threats for ICEI, associated with the rapid evolution of viral software, which poses a serious danger for many components of IEEU. Note that modern viruses are designed not only for Windows OS, but can also be dangerous for other systems in the IEEU structure, for example, for HDI and sensory subsystems (figure 1.3).

Modern computer networks of universities are usually associated with corporate information systems (CIS), and also have unlimited access to public networks. This increases the efficiency of the educational process implementation, but in parallel creates additional vulnerabilities, for IEEU, as well as for computerized OS control systems (for example, accounting systems for employees and students, accounting for material values, etc.). At the same time, such cyberattacks are quite realizable through the elements of interconnecting of IEEU with the local networks of student and teaching campuses, as well as with global networks, see figure 1.4.

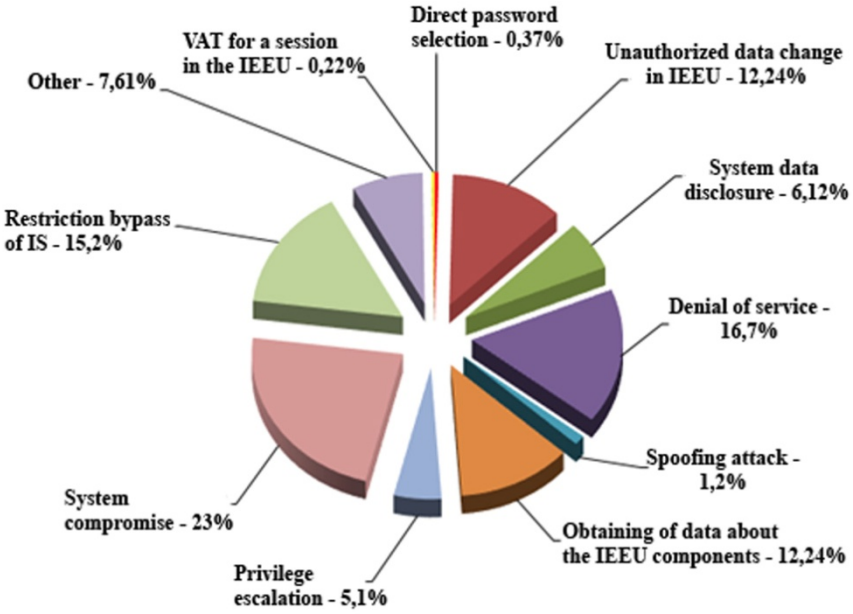

Figure 1.1 – Distribution of ICS vulnerabilities of public organizations

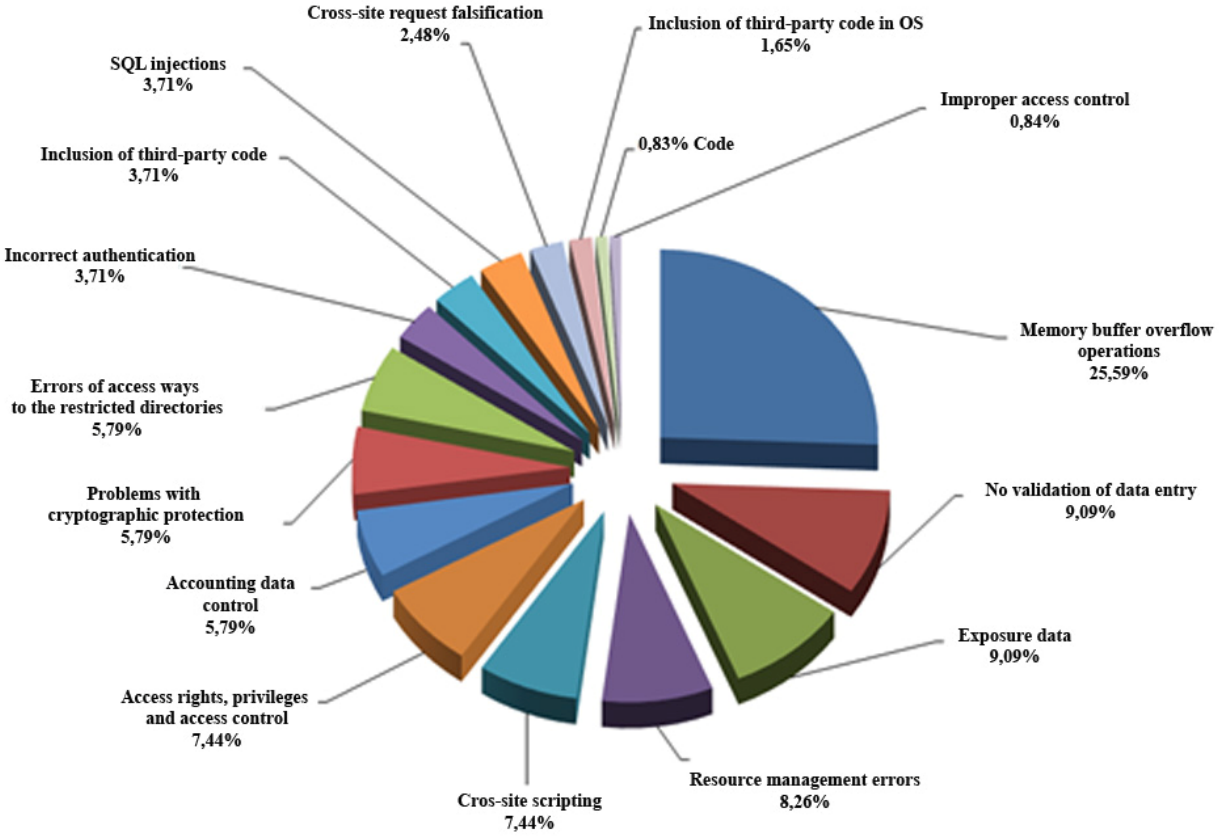

Figure 1.2 – Attacks on ICS of public institutions

Table 1.1 – Aims, objects and subjects of attacks on IEEU

Types of cyberattacks			
Cyber espionage - unauthorized transmission using hidden (undeclared) data communication channels, IP programs, etc.)	Cyber audit - development of cyber attack scenarios, hacker and "friendly" cyber attacks, search for vulnerabilities in the IEEU.	Cyber fraud - the "sale" of fake electronic documents, and etc.	Cyber sabotage - a decrease in productivity, including at the expense of the IEEU resources, in particular, till a complete stop of the educational process.
Objects of cyberattacks			
InformationSystemsof EI	Own or ordered software of EI	EI databases	Local network components
The objects of cyber attacks on IEEU are: IS of EI, distance education systems, database servers, data of students, staff, support staff, etc.			
Attacking side			
Novice hackers, professional hackers, competitors, insiders, organized crime groups, etc. At the same time, the level of technical equipment and competence of the attacking side can be quite high.			

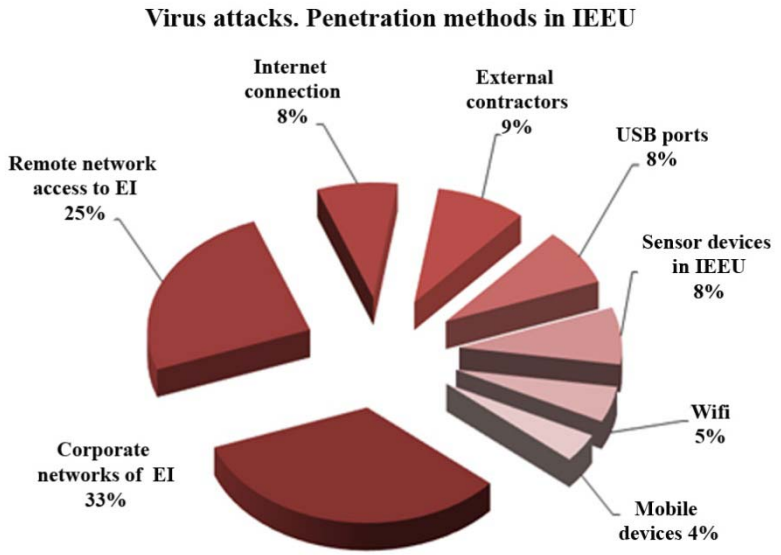

Figure 1.3 – Virus attacks on ICS of publicin stitutions (penetration methods)

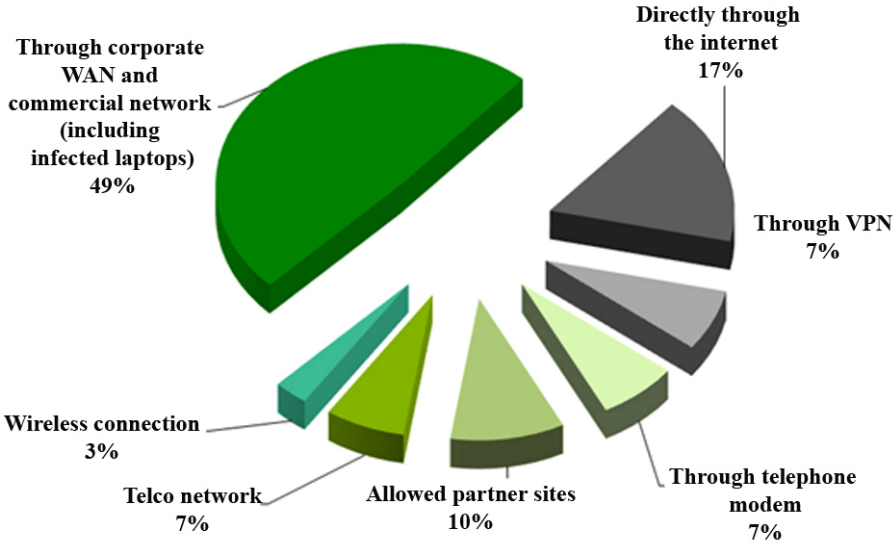

Figure 1.4 – Sources and channels for the development of attacks on IEEU and on the control systems of educational institutions

Analysts of various companies that deal with IS and CS issues, including for government organizations (including major EU and US universities), on the basis of long-term cyber incident statistics, cite such data on the distribution of ICS vulnerabilities. Web-applications account >40% of vulnerabilities, about 23% for server software, > 25% for client software and about 11% for operating systems [12], see figure 1.5.

Similar data are cited by other sources. According to [93, 95, 96] approximately 40% of all detected in 2010–2018 vulnerabilities of ICEI were accounted for Web-applications.

For several years, analysts in the field of IS and CS have fixed a trend indicating a steady increase of the amount of cyber incidents and cyberattacks in IEEU, figure 1.6.

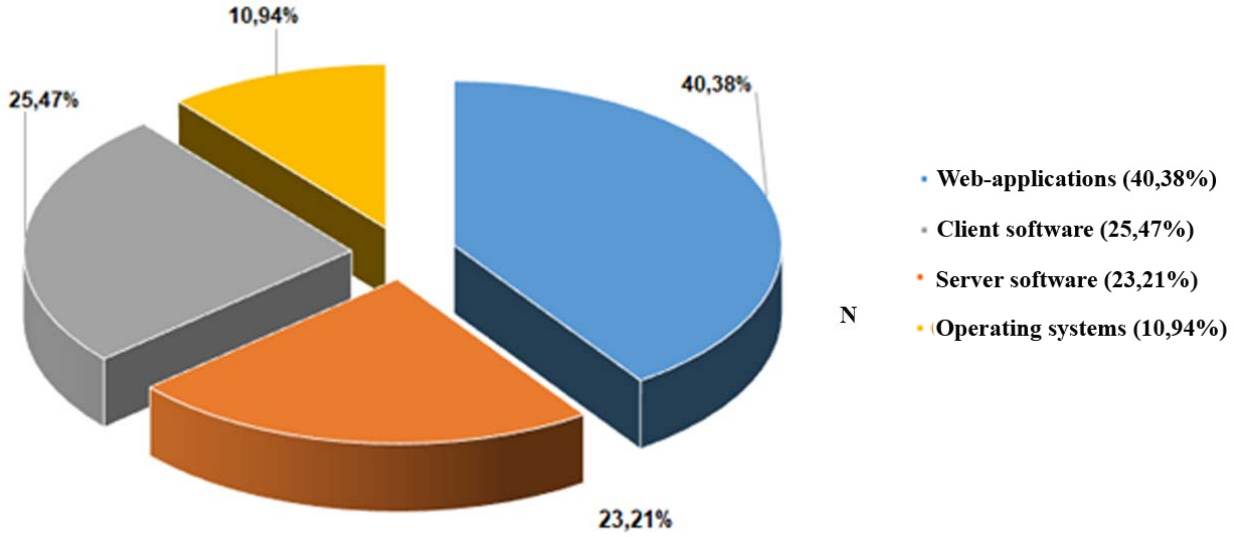

Figure 1.5 – Distribution of vulnerabilities by the type of application in IEEU
(For the period 2010-2018)

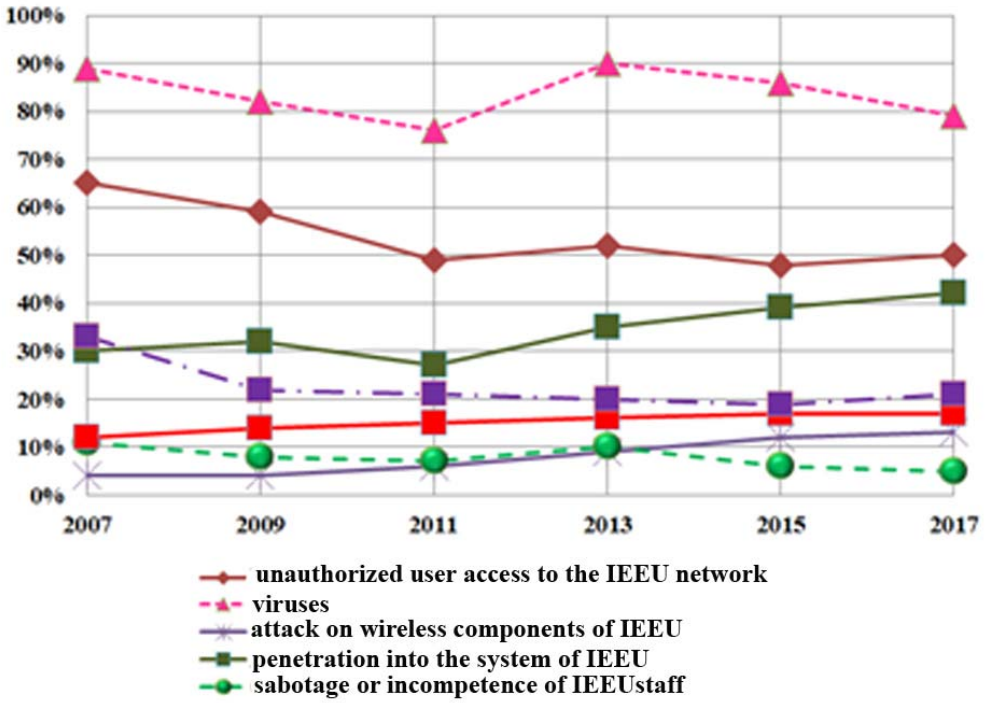

Figure 1.6 – Cyberthreats dynamics for ICS of EI
[According to 7, 11, 18]

This, in particular, can be explained by the increase of the amount of local networks of universities and other EI that are connected to public networks [12, 13].

In publications devoted to the problem of evaluating the security of IEEU [10, 12] it is noted that in addition to the technical tasks on protection of the information circulating in ICSU, it is necessary to analyze periodically information risks and to monitor the effectiveness of the implemented measures aimed at ensuring IS and CS of the university. These procedures allow to consider:

- the variability of requirements in the tasks of information protection (for example, from content protection to protection of personal information of employees and students);
- the potential possibility for the emergence of new cyberthreats and vulnerabilities in ICSU;
- the decrease of the effectiveness of already implemented measures for information protection over time;
- the decrease of the reliability of information processing in IEEU by physical obsolescence of the equipment and software.

An active implementation and widespread use in universities and other educational institutions of wireless networks, including sensor networks and technologies [13, 14], has created new vulnerabilities for the cyberattacks class - denial of service.

In addition, as was shown in [10, 14], the sensor nodes are often least protected from unauthorized access (UAA). At the same time, their resources and service life depend on the power supply, the amount of on-off cycles, which in turn may become a target for hackers. Therefore, an attacker can use such restrictions in order to obtain full control over the IEEU sensor node, for example, over the terminal through which tuition fee is paid or for other services provided at the university (payment for a hostel, Internet services, a gym or other). Sensor nodes are also can be easily compromised, in particular, by DoS-attacks.

During the development and modernization of CICS, there are implemented modules and components of third-party suppliers in them, in particular, sub-components can be responsible for IS of CICS. But, during such modernization the procedure of preliminary testing of their cyber-security is not performed, such components may be vulnerable to potential attacks.

We also note the data of the researches [9, 15], in which there were considered the problems of reducing the complexity of successful cyberattacks aimed at ICS of state structures. In particular, it is noted that the complexity level of successful attacks has decreased from a maximum value of more than 87% in 2004, to 46% in 2018, see figure 1.7.

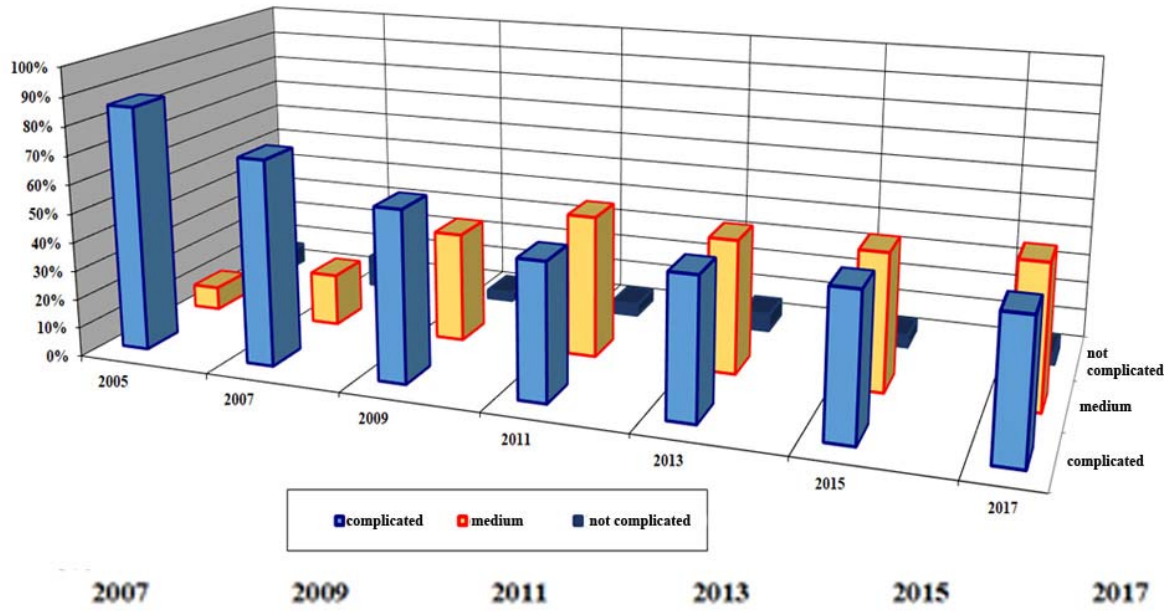

Figure 1.7 – Requirements growth dynamics for the level of cyberattacks complexity

However, for the same period of time, the amount of vulnerabilities of medium complexity in ICS has increased from 5% to 44%. Attacks on complicated vulnerabilities in ICS remain approximately at the same level for the last decade and do not exceed 3-4 4% [12].

Details in carrying out such an analysis in comparison with past results will ultimately determine the allowable risk levels for IS and CS of IEEU [15].

The approaches to solving the above problems [15,16], described in many literary sources, at one time allowed to make significant progress in solving them for commercial enterprises and organizations. However, EI with their specific of access organization to information resources cause a slightly different specifics of the organizational and technical control of IS and CS.

It should be noted that many EI (schools, colleges, universities, student campuses, libraries, etc.) still retain their traditional approach to solving problems of financing of means and information protection systems (IP) and cybersecurity (CS) [1, 2]. Most of the funding strategies to the CS systems involve only the allocation of funds for anti-virus programs and for relatively uncomplicated network protection tools [2, 3]. This is a very simple financial strategy for cyber protection of EI. Even experienced administrators of information and cyber security services are not always ready for the worst case scenario during cyber-attacks on computer systems and EI networks [2, 3]. The information protection side needs to shift its attention to changing traditional approaches on CS means (CSM) financing. For example, at the stage of choosing the financial component of CS strategy investment the change to the policy, which involves the detection and blocking of potential hacks of computer systems and networks of ICTS of EI [4].

In works [15, 17] there is noted that today international investment projects in the field of education and, in particular, in the field of digital information and educational platforms, have become common practice of international cooperation. In our opinion, such investment projects must necessarily involve a deep analysis of the financial strategies for ensuring the cybersecurity of EI and their joint information and educational environment. As many specialists of information protection (IP) note, CSM of educational institutions, in particular, large international, public and private universities should not only ensure the safety of information files and data, including confidential, but also guarantee the impossibility of external unauthorized penetration into IEE of EI [1-3]. The constant increase of the amount of cybercrimes in the world only reinforces the need to increase financial investments in CSM [4–6], in particular for EI.

We should note that to the protected information, that is stored and circulate in the EI, there can be attributed [2, 4, 7]: personal data of students, teachers, employees; digitized information representing the intellectual property of the educational institution; information arrays that provide the learning process (for example, multimedia content, databases, training programs); others

This information can act as an object of theft or distortion from external (internal) computer intruders (CI) or from hooligan motives, from students or employees.

Taking into account the interpretation of IEEU, given by different authors, it is possible to modify its structure taking into account the problems of ensuring cybersecurity [17]. Therefore, is there is proposed such a protected structure of IEEU and, accordingly, the information and educational space of the university, see figure 1.8.

Naturally, the construction of such a complex organizational structure as protected IEEU (hereinafter - IEEU) requires sufficiently large financial resources, which still need to be properly managed.

The procedure for investing in innovative projects, in particular, in the development of digital educational technologies with a focus on formation of the information and educational environment (IEE) of EI, is often characterized by a high degree of uncertainty and riskiness in the tasks of ensuring the cybersecurity of EI. The landscape of cyberthreats that has changed in recent years [5, 6] has fundamentally influenced the attitude to the problems of CS of many EI [1, 2]. First of all, this was due to significant potential vulnerabilities and cyberthreats for IEE of EI, to the emergence of new classes of cyberattacks, to the widespread use of wireless data transmission technologies, etc. With the rapid implementation of digital technologies in education, not all investors, for example, at the creation private and including large international universities in the Russian Federation, Ukraine, and Kazakhstan, paid due attention to the problems of CS of IEE EI [1, 2, 5]. We also note that not many publications in this field contain a description of models related to finding different variant strategies in mutual financial investment of EI in CS [3, 4].

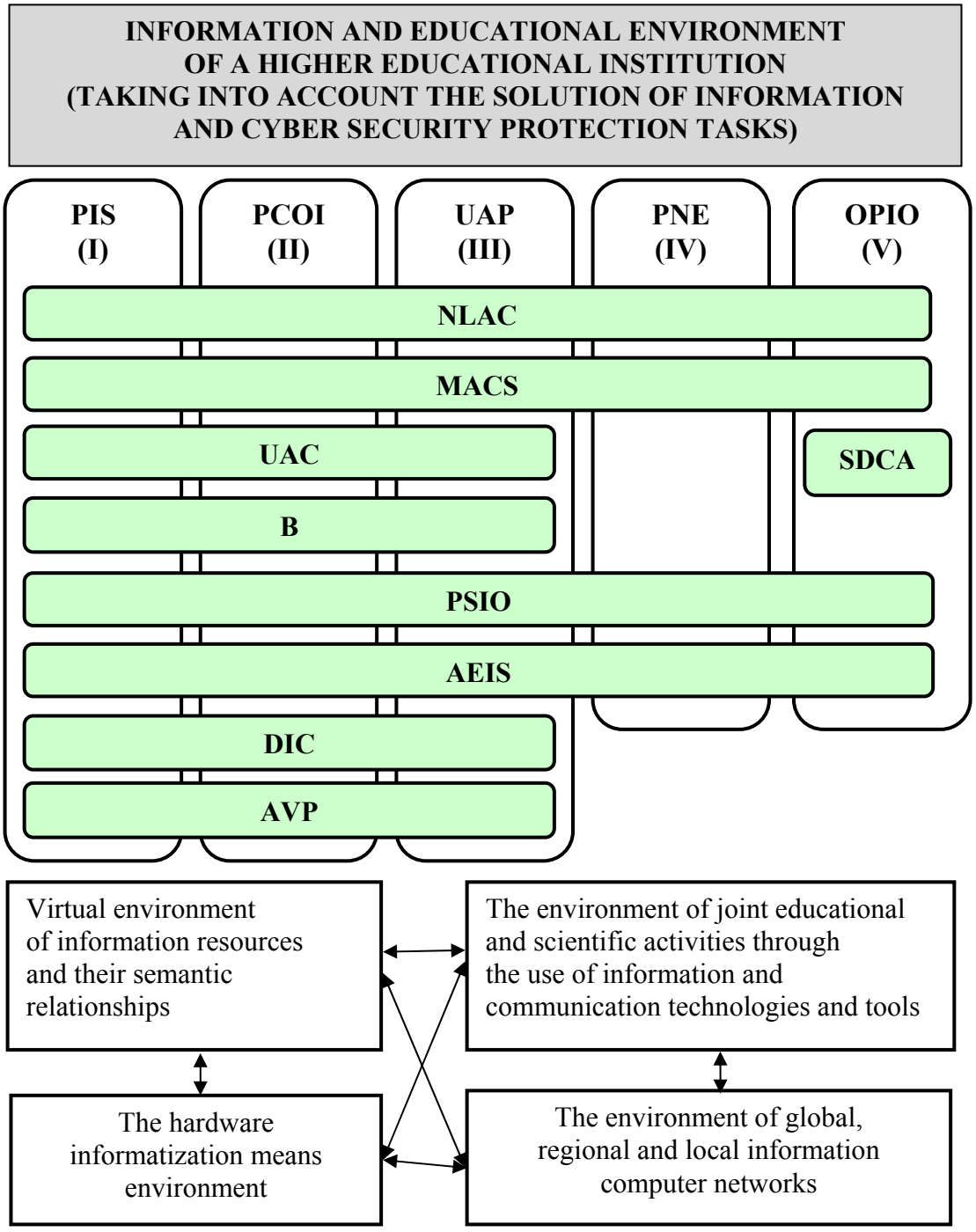

Figure 1.8 – The structure of the protected information and educational environment of the university

The following notations are accepted: AVP – antivirus protection; DIC – data integrity control; AEIS – audit of events of information security; PSIO – physical security of information object; B – backup; UAC – user access control; SDCA – subsystem of detection of cyber attacks; MACS – Monitoring and; analysis of cyber security; NLAC – Network-level access control.

CS of IEEU perimeters: PIS (I) – The perimeter of the information system; PCOI (II) – Perimeter of control of object of informatization; UAP (III) – User Access Perimeter; PNE (IV) – The perimeter of the network equipment; OPIO (V) – The outer perimeter of information object.

In order to improve effectiveness in evaluating various investment projects CSM of EI, and the subsequent decision-making, related to investment, it is necessary to use modern information technologies [5]. For example, technologies that are based on the use of decision support systems (DSS) [1, 2].

The filling of the information and algorithmic component of the DSS can be implemented by introducing blocks that contain algorithms for mathematical models for CSM of EI investment.

We should note that despite the commonality of the taskson CS for various informatization objects (hereinafter IO, it is accepted that IO can be IEEU, an automated control system for complex production control or a banking system), each of them has its own specificity of cyberthreats [1-5]. However, a common initial task at the creation of effective protection systems and CS of any IO remains the task of examining a specific protection object, forming models of a potential intruder (computer intruder - CI) and cyberthreats [1-5]. The implementation of the above steps will ultimately provide adequate requirements for information security systems (ISS) of IO and IEEU, as a special case.

In the conditions of increasing complexity of cyberattack scenarios on IEEU, information security analysts at universities and other educational institutions need to respond fairly quickly to cyberattacks, threat anomalies. This makes it urgent to search for new ways to improve the effectiveness of decision-making in tasks of respond to attempts of destructive interference by CI or unfair university staff in IO work. And in this situation, various intellectual decision support systems (IDSS) and expert systems (ES) can play a significant role in the tasks of ensuring cyber protection of IO [5-7].

The mathematical component of the IDSS and ES in the tasks of CS are the various models and algorithms that enable professionals to intellectualize decision support. As part of the research, there was considered the possibility of synthesizing analytical models for the main types of unauthorized access to the IEEU resources. The possibility of describing functional models of cyber protection systems of IEEU in terms of Petri network theory [7, 8] seems quite promising. Such a presentation will allow IS and IP analysts to detail the threats in protected IEEU. In addition, in the future, it is possible to determine the states that potentially determine the vulnerability of IO to the new cyberthreats. There is also considered the perspective of using this model based on Petri networks (and Petri – Markov networks) and colored Petri networks as a mathematical and algorithmic component, designed by IDSSat analyzing cyberthreats for various IOs. In our opinion, these judgments make our work relevant and increase the effectiveness during the creation of IDSS in the tasks of IS and CS for various IOs.

Consequently, the task of developing new mathematical models for DSS, which will allow adequately to describe the actual processes of CS investment, is an urgent task. This will allow more sensible to choose approach of funding strategies for CSS of EI.

1.2. Review and analysis of previous researches in the field of cyber protection of the information environment of educational institutions. To the theoretical researches of the cyber protection problem of information and communication systems (ICS) of state structures, including IEEU, there were devoted a great number of works of scientists from the CIS countries: Bidaybekov EY. [19], Fedorov A [1], Shafeev DE. [2], Zhankalova ZM. [3], Khokhlov YE [4]., Yakovlev AS [7], Kubieva TS. [14], Tleuberdiyeva G. [17].

However, in Kazakhstan and other CIS countries these publications are rather limited in scope or are very fragmented, being limited only by theses of reports on the topic “the needs for cyber protection of educational institutions”. Theoretical studies and research results are presented in some publications [4, 8, 13-15], and in others - experimental data or results of simulation modeling [15]. A separate segment of research is devoted to the problems of developing hardware and software means for IS and CS for EI [15, 18, 19].

To the researches of the effective strategies choice for financial investment in CS, in particular for EI, there were devoted a fairly large amount of publications [4-6].

Among the IS and CS models, the Gordon-Loeb (GL) model [8, 9] is the most thorough and widespread. The purpose of this model is to solve problems associated with determining the optimal amount of investment to information protection. The key point in the GL model is the implementation and development of the vulnerability function, which determines the level of IS and CS for the considered informatization object, in particular for IEEU. An informatization object can have various forms – a list of users, a book of accounts, a strategic development plan, a website, and etc. Security enhancement may occur in the direction of protecting confidentiality, integrity, authenticity, reliability, availability of user authorization, etc.

The model is static in its structure. Consequently, decisions and results occur simultaneously, and dynamic effects, including the dependence of money on time, are not taken into account.

Considering that investments in the means and methods of IS and CS are ineffective with sufficiently small and sufficiently large values of vulnerability, the authors of the GL model, as well as several works [8, 9] who developed the ideas embodied in the GL model [16, 17], noted the following circumstance. Many authors believe that the first task of control the separation of objects into low, medium and high levels of vulnerability should be addressed at the preliminary design stage. However, at the same time, the authors of the GL model [18], similar models noted its disadvantages:

1. There is no simple procedure for determining the possibility of an attack and the vulnerability of information arrays.

2. It is problematic to determine the potential losses from the security violation of the protection perimeters and cybersecurity of the informatization object. (For ourselves, we note that for IEEU these perimeters of IS and CS are rather conditionally enough).

3. The complexity of the research results implementation on a specific object.

4. It does not take into account how the attacker will change his strategy at making additional investments for protection, that is, there is no analysis of the opposition in a dynamic mode.

Despite the fact that the GL model has been widely recognized and has been developed in many works over a decade since its publication, most of the posed problems have not been solved till today. The undeniable merit of the authors of the model is that for the first time they thoroughly examined the problem and identified the vulnerability function, which is a key oneat considering the confrontation in the information sphere.

Determination of the function form expresses the vulnerability of a dynamic system, and is a key task in the mathematical modeling of information opposition, and the work of many researchers has been devoted to this problem [18].

According to the history of the problem the confrontation of the two sides was firstly thoroughly examined by specialists of the RAND Corporation at the end of the Second World War during the development of the mathematical foundations of military planning. The model of confrontation of the two sides, developed within the framework of the RAND company, is the model of Gross [12, 15], designed in order to simulate tactical military operations. According to this model, the conflicting sides have the resources $X$and$Y$, and the result of their opposition is determined by the target function, which linearly depends on the difference of the invested resources and which leads to the task of linear programming. The task of Gross, which arose during the planning of military operations, has a number of differences from the considered problems. Firstly, the target function is discrete, since it determines the amount of units that broke through the defense or destroyed an attack or defense. Secondly, these units in each confrontation episode are the same for attack and, accordingly, for defense.

The uniformity of objects greatly simplifies the solution of the problem, but limits the confrontation conditions. However, the main disadvantage of the Gross model is the piecewise linear character of its target function, which, of course, cannot correspond to real conditions. For this reason, the Gross model, taking into account its simplicity, is used only to approximate the target function and to obtain results at the first approximation [4, 12, 18].

Another mathematical model, that makes it possible to calculate the level of losses due to the realization of threats,and which depends on the amount of costs on IS and CS, is the model described in [11]. The purpose of the researches [12] was to assess the stability of the technical information protection complex (TIP) over time using known probability distributions [4, 5].

In the absence of financial investments in protection or its modernization, the probability of reliability, security is zero regardless of time. This model allows to establish the dependence of the protection probability from the most effective investment.

The main difficulties at the creation of the model are connected with the collection of statistical data on the hacking results (and the need for the fact of the protection hacking itself), since such a protection system cannot be used afterwards. In this regard, the author [13, 21] developed a method for determining the probability of reliability of TIP based on actual hacking attempts, which allows to evaluate the probabilistic reliability of single protection systems and at its installation on several objects (for example, installation of an antivirus program on several computers allows to predict not only an attempt, but also

the time at which hacking is possible on other computers) [16]. The disadvantage of this method is the need to know the effectiveness of TIP, which in this case is obtained as a result of analysis the consequences of a real hacking of the system.

As a result of the researches conducted in [17, 19], the authors showed that the parameter that determines the properties of TIP can be not only a constant value, but also a function. Moreover, this function will depend on hacking attempts and on the time when such attempts take place, for example, at the selection of passwords during the user authentication procedure in the informatization object network []. According to the researches there were obtained functions that allow to calculate the frequency of hacking attempts.

The Glushak-Novikov model [17, 18] is aimed at optimal placement of protection mechanisms between the components (objects) of the system, which will ensure the maximum level of security.

The search for the optimal set of protection mechanisms that ensures the minimum risk of information loss is carried out using the example of a district offices system of theinformatization object distributed territorially (the author considered an example of a bank branch) [10, 20]. The amount of information in each department is proportional to the potential amount of customers, that is, to the amount of residents in the district. The probability of individual threats realization, as well as the cost and effectiveness of each of the protection mechanisms, is determined by the method of expert evaluation. It is assumed that the probability of a threat realization for each object is the same and depends only on the type of the threat. Considering the various combinations of protection elements for each of the territorial branches, there are calculated the total damage for the entire system (which characterizes the degree of risk) and the optimal set of protection elements for each branch. In this case, there is made a check of the conditions for imposing restrictions on the total cost of the protection system.

Calculating the total risk, the problem of the size of the cross-section equations, which express the amount of damage from the realization of various types of threats (these events are considered compatible), remains open.

To the use of the “attack-protection” economic value models for risk assessment and for the researches on the investment effectiveness in information security there is devoted the work of O.E. Arkhipov [4, 5]. In order to determine the risk probability parameters in these models, there are used certain characteristics of motivational value and economic and financial relations characteristic for the “attack-protection” situation in the information sphere. In particular, the there is considered the situation arising from the realization by the attacking side *A*(the attacker) of the threat *T*regarding some information resource *I*, which belongs to the side *B*.

The describedin [9, 20] models are proposed to be used in order to calculate directly the risks of any particular organization if there is a real opportunity to analyze and to quantify the economic and cost characteristics of the information threat realization. Output data for these assessments can be obtained by performing a survey (audit) of the organization’s information security state in accordance with the guidelines and recommendations of risk management standards with certain additional information. Static-time assessments can be developed into dynamic ones that change their values in time according to the accepted economic and cost attack scenarios [5].

The economic and cost-based “attack-protection” models also provide an opportunity, on the basis of specific information about a real organization, to check whether the funds invested in the information security of this organization are sufficient [6].

To theresearches of cyber attacks on information systems there is devoted the work of Khoroshko V.A. [10]. An assessment of the attacker's capabilities in cyber attacks is carried out using game analysis methods [15].

Formalizing the optimal cyber attack cycle on the information sphere there is supposed the operating of the equilibrium concept of Nash B.[15].

We should note that this model does not take into account the impact of investments on the optimal solution choice, however, the researchers demonstrate how the developed game analysis methods allow to evaluate both single and group cyber attacks.

This allows to obtain guaranteed and reliable assessments of the level of information security from cyber attacks on the information sphere, for example, of an educational institution [9].

The development of economic relations and the information sphere, particularly, in the field of education, leads to an increase in competition, to an increase in the volume and cost of information, as well as potential losses from its leakage, to an increase in the amount of information objects (in IEEU this is especially noticeable and dynamic),tothe frequency of cyber incidents. At the same time, the opposition conditions are constantly changing, reflecting the dynamic interaction of two opposite sides - the side of information protection and the side of the attackers. Changes in the strategy and tactics of the cyber protection side cause new attacks on information resources, which, on the one hand, show the opponent's intentions, on the other hand, point to weaknesses of the protection side, which are usually targeted by attacks or other attempts of destructive intervention. Other reasons for changes in approaches of IS and CS of IEEU can be factors related to the "obsolescence" of information, to the introduction of new information and additional resources, to the redistribution of information resources between objects, to the occurrence of new connections between them.

The antagonistic confrontation of the two sides (the protection and attack sides) in the information sphere is characterized by the fact that the protection side is usually in uncertainty about the actions and financial capabilities of the enemy (hacker). At the same time, the attackers have some idea about the structure of the protection system and can direct their efforts towards breaking the weakest points of the security system. That will give the attacker the greatest effect. The distribution of protection resources to blocking various types of threats can be carried out both in active mode – ahead of the opponent's actions, and in adaptive one with aninvestmentdelay when the direction of possible attacks is clear.

We should note that the need for dynamic resource control is due to the following reasons:

- the uncertainty of the opponent's action variants, namely the focus of his efforts to obtain information and the scale of these efforts, which in particular depend on the financial hackers' resource component, spent on hacking;
- the changes in both internal and external confrontation conditions - the information cost, its distribution among objects, the direction of enemy attacks, the occurrence of new attackers;
- a change of the information system state (IEEU is considered as a special case), in particular, a change in its weakest unit after detection of the attacks target and the adoption of appropriate measures by the protection side.

Analysis of scientific works on mathematical modeling of information protection systems showed that the main efforts are focused on determining the amount of investment in protection (table 1.2).

Several works are devoted to theproblems of distribution of these investments among the protection objects. In addition, existing developments [9] rarely take into account the impact of possible actions of the attacker and their consequences on the indicators and characteristics of the system.

Therefore, the conducted analysis of the workson the subject under study showed that the task of efficient using of limited financial resources in order to protect information of business entities and educational institutions in particular is becoming increasingly important and significant [15, 16, 20, 21].

Table 1.2 – Comparative characteristics of mathematical models of investment in information and cybersecurity of the informatization objects

Compared criteria / Models	Security resources are taken into account	Attacking resources are taken into account	The cost of the individual protection mean is taken into account	Object vulnerabilities are taken into account	Optimization of resource distribution between protection objects	Calculation of the optimal solution in the dynamic mode
Gross model	+	+	–	–	+	–
Gordon-Loeb model	+	–	–	+	–	–
Zadirako model	+	–	–	–	–	–
Glushak-Novikov model	+	–	+	–	+	–
Zhurilenko model	+	–	–	+	–	+
Arkhipov model	+	+	+	+	–	+
Khoroshko-Khokhlachova model	–	–	–	+	–	+

In addition, in conditions of uncertainty, when the actions and financial resources of the attacking side can be assumed only with a certain probability, the search for the optimal distribution of limited resources among the information protection objects through the use of game-theoretic methods and taking into account the dynamics of opposition conditions will reduce financial losses from information leakage to a minimum.

The development of computer systems and information technology has given a rise to a separate concept of works on optimizing investment in CS. This research concept is based on the extensive use of expert systems (ES) [7-9] and DSS [10-12] in the tasks of determining rational investment strategies in the field of CS. We studied quite a lot of works in this area and came to the conclusion that most of these publications [12] do not contain specific decisions on the choice of rational strategies for mutual financial investment in CS of EI.

Also, as follows from the conclusions of [8, 9] and [11, 12], the use of ES and DSS in order to automate procedures for choosing rational investment control strategies for CS is not always accompanied by clear recommendations.

These circumstances led to the problem associated with the need to develop new models for DSS in the tasks of determining rational strategies for mutual financial investment in CS of EI.

Based on previous experience and approaches presented by the authors in earlier publications on this topic [9], as well as works of third-party authors [14] that are close to the research methodology, we can state that a rather effective approach in order to solve this class of problems is to use methods of the theory of differential qualities games with several terminal surfaces [4-7].

Therefore, the analysis of publications on this topic confirmed the relevance of the problem of the further development of models for DSS in the tasks of continuous mutual investment in CS of EI. The last one is especially important in cases where it is necessary to develop clear recommendations for investors. But there is no need to apply complex mathematical calculations, since most of the computations are done by computer programs.

In works [1-6] there were presented the results of researches on the use of Petri networks for describing the threat model of CS of IO. And although these works have made an undeniable theoretical contribution in this area, in our opinion, the models proposed by the authors are somewhat difficult to implement programmatically, in particular in the IDSS and ES on IP and CS of IO.

On the basis of the works [2, 3] it is possible to construct threat models using a fairly visual tabular form of displaying threats at updating the task of IO security assessment. But as mentioned earlier, this approach to the development of threat models is laborious. And besides, the growth in the amount of threats makes such a tabular presentation format difficult to understand, especially for specialists with small experience in the field of CS.

Petri networks (and Petri – Markov networks) were also successfully used to describe intruder models [4]. However, the authors did not consider the possibility of adjusting the intruder model (CI), in particular, by combining it with models based on the graph theory, which would more accurately describe the transition states in the process of probable overcoming of the cyber defense perimeters (borders) of CS by CI for a particular IO.

In the works [13, 19, 20] the ISS models for various IOs were considered as a sequence of elementary operations that were pre-allocated on the Petri network, from which a cyber attack is possible. The models made it possible to calculate the probabilities of the implementation of different attacks over a given period of time. However, the models considered in [13] did not allow the calculation of temporal characteristics during the process of implementing new cyber threats.

In the works [17, 21] there were also proposed the models based on Petri networks and describing the processes of realization of threats in information systems (IS). And although these models make it possible to assess many of the parameters of IO security, in particular, the possibilities of threats, the time for threats, the consistency of the CI actions seems to be incomplete. In particular, in these works there has not been studied the problem of resolving conflict situations that arise when IS states change during attacks belonging to different classes. This circumstance, in our opinion, limits the practical applicability of these researches.

Therefore, the addition of existing methods of detecting and analyzing threats, as well as intruder models on the basis of algorithmization and visualization of Petri networks can be an effective tool for

predicting the security state and new threats for specific IOs. This will significantly simplify the understanding for new cyber threats and in the future it will be possible to use the proposed approaches by analysts of the IP and CSservices of different IOs.

1.3. Conclusions and statement of research objectives. In order to achieve the aim of the research it is necessary to solve the following tasks:

- to develop a model for a decision support system for searching the investment control strategies for various ratios of the investment process parameters in the cyber security systems of educational institutions;
- to develop a computer program "Decision Support System for Searching the Investment Control Strategies in Cyber security Strategies of Educational Institutions";
- to perform computer simulations for different investment strategies, in order to verify the adequacy of the model;
- to develop a conceptual model of the adaptive cyber protection control of an informatization object (for example, IEEU) using the apparatus of Petri networks;
- to develop models for user tasks distribution in the IEEU computer networks;
- to complement access control methods in the context of reconciliation of access rights in IEEU.

Л. Қыдыралина[1], Б. Ахметов[1], В. Лахно[2], А. Адранова[1]

[1]Абай Атындағы Қазақ ұлттық педагогикалық университеті,
Алматы, Қазақстан,
[2]Украинаның биоресурстар және табиғатты пайдалану ұлттық университеті,
Киев, Украина

УНИВЕРСИТЕТТЕРДІҢ АҚПАРАТТЫҚ БІЛІМ БЕРУ ОРТАСЫН ҚОРҒАУДЫ ҚАМТАМАСЫЗ ЕТУ СФЕРАСЫНДАҒЫ АЛДЫҢҒЫ ЗЕРТТЕУЛЕРГЕ ШОЛУ ЖӘНЕ ТАЛДАУ

Аннотация. Жұмыста университеттердің ақпараттық білім беру ортасын қорғауды қамтамасыз ету сферасындағы алдыңғызерттеулерге шолу және талдау жасалған. Әлемде көптеген өнеркәсіптері дамыған мемлекеттерде цифрлық білім беру жүйесінің дамуындағы артықшылығы тек қана педагогикалық қызмет облысындағы мамандарға ғана емес, ақпаратты қорғау және киберқауіпсіздік проблемаларын ескере отырып ақпараттық технологиялар мамандарына да сәйкес технико-методологиялық қолдауды талап ететіні көрсетілген. Университеттердің ақпараттық-коммуникациялық жүйелерінде сақталатын және айнала отырып қорғалатын мәліметтерге атап айтқанда: оқушылардың, оқытушылардың, ғылыми қызметкерлердің, көмекші қызметкерлердің жеке мәліметтері; оқу орнының интеллектуалды жеке меншігі ретінде қарастырылатын цифрланған ақпарат, оқу процесін қамтамасыз ететін ақпараттық массивтар (мысалы, мультимедиялық контент, берілгендер базасы, оқыту бағдарламалары); т.б. жататыны көрсетілген.Осы ақпараттық ресурстар ішкі және сыртқы компьютерлік қаскүнемдерден немесе бұзақылық әрекетпен оқушылар немесе қызметкерлер тарапынан ұрлауға немесе бұзуға болатын объект ретінде қарастырыла алатыны негізделген.

Көптеген мемлекеттерде ақпараттық ресурстарға қол жетімділікке қалыптасқан жаһандану тренді заманауи жоғары оқу орындарының қызметтерінің барлық сферасына жаңа цифрлық және ақпараттық-коммуникациялық технологияларды енгізу есебінің өзектілігін көрсететіні дәлелденген. Оқу мекемелерінің киберқауіпсіздік жүйелерін қаржыландыру процесінің параметрлерінің түрлі қатынастары үшін қаржыландыруды басқару стратегияларын табу бойынша шешімдерді қолдау жүйелері үшін модельдерді әзірлеу бағытында зерттеудің өзектілігі негізделген. Оқу мекемелерінің киберқауіпсіздік стратегияларына қаржыландыруды басқару стратегияларын табу есебін компьютерлік қолдау арқылы шешу қажеттілігі көрсетілген. Обоснована необходимость разработки концептуальной модели адаптивного управления киберзащитой объекта информатизации на примере ИОСУ. Университеттің ақпараттық білім беру ортасы мысалында информатизация объектісін киберқорғауды бейімделген басқарудың концептуалды моделі нәзірлеу қажеттілігі дәлелденген.

Түйін сөздер: киберқауіпсіздік, ақпараттық-коммуникациялық орта, оқу мекемелері, ойындар теориясы, шешімдерді қабылдауды қолдау, қаржылық стратегияларды таңдау.

Л. Кыдыралина[1], Б. Ахметов[1], В. Лахно[2], А. Адранова[1]

[1]Казахский национальный педагогический университет им. Абая, Алматы, Казахстан,
[2]Национальный университет биоресурсов и природопользования Украины, Киев, Украина

ОБЗОР И АНАЛИЗ ПРЕДШЕСТВУЮЩИХ ИССЛЕДОВАНИЙ В СФЕРЕ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ УНИВЕРСИТЕТОВ

Аннотация. В работе проведен обзор и анализ предшествующих исследований в сфере обеспечения защиты информационно-образовательной среды университетов (ИОСУ). Показано, что приоритетность развития цифровых систем образования во многих промышленно развитых государствах мира требует соответствующей технико-методологической поддержки специалистов не только в области педагогической деятельности, но и информационных технологий с учетом проблематики кибербезопасности и защиты информации. Показано, что к защищаемым сведениям, которые хранятся и циркулируют в информационно-коммуникационных системах университетов, в частности относятся: персональные данные учащихся, преподавателей, научных сотрудников, вспомогательного персонала; оцифрованная информация, представляющая интеллектуальную собственность учебного заведения; информационные массивы, которые, обеспечивают учебный процесс, (например, мультимедийный контент, базы данных, обучающие программы);др. Обосновано, что данные информационные ресурсы могут выступить как объект хищения или искажения со стороны внешних (внутренних) компьютерных злоумышленников или из хулиганских побуждений, со стороны учащихся или сотрудников.

Обосновано, что сформированный во многих странах тренд на глобализацию доступа к информационным ресурсам делает релевантными задачи внедрения новейших цифровых и информационно-коммуникационных технологий во все сферы деятельности современного вуза. Обоснована актуальность исследований в направлении разработки моделей для систем поддержки решений по нахождению стратегий управления инвестированием для различных соотношений параметров инвестиционного процесса в системы кибербезопасности образовательных учреждений. Показана необходимость компьютерной поддержки решения задач по нахождению стратегий управления инвестированием в стратегии кибербезопасности образовательных учреждений. Обоснована необходимость разработки концептуальной модели адаптивного управления киберзащитой объекта информатизации на примере ИОСУ.

Ключевые слова: кибербезопасность, информационно-коммуникационная среда, учебное заведение, теория игр, поддержка принятия решения, выбор финансовой стратегии.

Information about authors:

Kydyralina Lazat, PhD student, Abai Kazakh national pedagogical university, Almaty, Kazakhstan; Lazat_75@mail.ru; https://orcid.org/0000-0002-2836-0919

Akhmetov Bakhytzhan, Professor, Doctor of Technical Sciences, Abai Kazakh national pedagogical university, Almaty, Kazakhstan; bakhytzhan.akhmetov.54@mail.ru; https://orcid.org/0000-0001-5622-2233

Lakhno Valeriy, Professor, Doctor of Technical Sciences, National University of Life and Environmental Sciences of Ukraine; valss21@ukr.net

Adranova Asselkhan, PhD student, Abai Kazakh national pedagogical university, Almaty, Kazakhstan; aselhan.adranova@mail.ru; https://orcid.org/0000-0001-7233-4104

REFERENCES

[1] Fedorov A.I. (2018) Prioritetnye napravlenija nauchnyh issledovanij v oblasti informatizacii sistemy podgotovki specialistov po fizicheskoj kul'ture, sportu i turizmu. Registracionnyj No. 4188-Zh No. 2, 2017, 137 (in Rus.).

[2] Shafeev D.E., Kogaj G.D., Ten T.L. (2016) Sistema professional'nogo obuchenija IT-specialistov v Kazahstane // Nauchnyj al'manah.11-2: 285-288. (in Rus.).

[3] Zhankalova Z.M., Baktybaeva A.T. (2017) Ctepen' razvitija informacionno-kommunikacionnyh tehnologij v Kazahstane: k postanovke voprosa // Mezhdunarodnyj zhurnal prikladnyh i fundamental'nyh issledovanij. 9:14-18 (in Rus.).

[4] Bugubayeva R.O., Tapenova G.S., (2019) Regulatory aspects of public administration system of higher education in the Republic of Kazakhstan // Bulletin of National academy of sciences of the Republic of Kazakhstan. ISSN 2224-5294. 2019. Vol. 1, N 323. P. 151-160. https://doi.org/10.32014/2019.2224-5294.24 (in Eng.).

[5] Zavivaev N.S., Proskura D.V., Shamin E.A. (2016) Informatizacija obshhestva, kak osnova global'noj konkurentosposobnosti // Azimut nauchnyh issledovanij: jekonomika i upravlenie. 5 (2(15)) (in Rus.).

[6] Mihnev I.P., Mihneva S.V., Sal'nikova N.A. (2018) Informacionnaja bezopasnost' v Rossijskoj Federacii: sovremennost' i perspektivy razvitija // V sbornike: Obrazovanie i nauka: sovremennye trendy. Kollektivnaja monografija. Ser." Nauchno-metodicheskaja biblioteka". Gl. red. O. N. Shirokov. Cheboksary, 103-112 (in Rus.).

[7] Jakovlev A.S., Kolomejchenko A.S. (2017). Informatizacija obshhestva: kurs na novye orientiry // Upravlenie jekonomicheskimi sistemami: jelektronnnyj nauchnyj zhurnal. (8(102)) (in Rus.).

[8] Rezgui Y., Adam M. (2010) Information security awareness in higher education: an exploratory study // Comput. Secur. 27(7): 241-253. DOI: 10.1016/j.cose.2008.07.008 (in Eng.).

[9] Sultan N. (2010) Cloud Computing for Education: A New Dawn? // International Journal of Information Management. 30:109-116. http://dx.doi.org/10.1016/j.ijinfomgt.2009.09.004 (in Eng.).

[10] Conklin A. (2006) Cyber defense competitions and information security education: an active learning solution for a capstone course // In: Proceedings of the 39th Annual Hawaii International Conference on the System Sciences. HICSS. 9:1-6. IEEE DOI: 10.1109/HICSS.2006.110 (in Eng.).

[11] Schuett M., Rahman M. (2011) Information Security Synthesis in Online Universities // The arXiv preprint arXiv:1111.1771: 1-20. DOI:10.5121/ijnsa.2011.3501 (in Eng.).

[12] Mariusz N., Benton M. (2017) Cybersecurity cost of quality: managing the costs of cybersecurity risk management // [El. resource]. https://arxiv.org/ftp/arxiv/papers/1707/1707.02653.pdf (In Eng.)

[13] Jalali M., Siegel M., Madnick S. (2017) Decision making and biases in cybersecurity capability development: evidence from a simulation game experiment // [Electronic resource]. 1-34. https://doi.org/10.1016/j.jsis.2018.09.003 (in Eng.).

[14] Kubieva T.Sh., Ponomareva N.I., Kozbagarova G.A., Oskenbaj S.A., Lazareva E.A., Musahanova M.K. (2013). Analiz rezul'tatov sotrudnichestva Kazahstana s izdatel'stvom ELSEVIER po ispol'zovaniju informacionnyh resursov // Vestnik NAN RK. 2: 44-51 (in Rus.).

[15] Gordon L.A., Loeb M.P., Zhou L. (2016) Investing in cybersecurity: insights from the Gordon-Loeb model // J. Inf. Secur. 7(02): 49-59. https://doi.org/10.4236/jis.2016.72004 (in Eng.).

[16] Akhmetov B., Lakhno V., Boik Y., Mishchenko A. (2017) Designing a decision support system for the weakly formalized problems in the provision of cybersecurity // East.-Eur. J. Enterp. Technol. 1(2(85)): 4-15 DOI: 10.15587/1729-4061.2017.90506 (in Eng.).

[17] Tleuberdiyeva G., Naizabayeva L. (2016) Monte carlo method for simulation of the application process with the use of service-desk technical support // Bulletin of National academy of sciences of the Republic of Kazakhstan. ISSN 1991-3494. Vol. 1, N 359. P. 32-39.

[18] Lakhno V., Boiko Y., Mishchenko A., Kozlovskii V., Pupchenko O. (2017) Development of the intelligent decision-making support system to manage cyber protection at the object of informatization // East.-Eur. J. Enterp. Technol. 2/9(86): 53-61. DOI: https://doi.org/10.15587/1729-4061.2017.96662 (in Eng.).

[19] Bidaybekov E.Y. (2002) About the training of specialists on informatics and informatization of education in the Republic of Kazakhstan // Technology of higher education in the XXI century: problems and prospects of development: collection of materials of the international scientific-practical conference – Aktobe: ASU named after. K. Zhubanov. P. 62-65 (in Rus.).

[20] Nurgaliyeva K.K., Suleev D.K., Tusubaeva Zh.M. (2002) Technology of distance learning organization: Monograph. Almaty: Republican Center for Informatization of Education, 50 (in Rus.)

[21] Akhmetov B.S., Gnatyuk S., Zhmurko T., Kinzeryavyy V., Yubuzova Kh.(2018) Experimental research of the simulation model for deterministic secure communication protocol in quantum channel with noise // Reports of the National academy of sciences of the Republic of Kazakhstan. ISSN 2224-5227. 2018. Vol. 5, N 321. P. 5-11. https://doi.org/10.32014/2018.2518-1483.1 (in Eng.).