Innovative activity of universities and the formation of entrepreneur universities of the innovative type is one of the forms of integration of the higher education systems of countries into the world educational and scientific space, support of their competitiveness. Based on the separation of interaction between universities and the economy and society, an evolutionary model of the university's interaction with stakeholders was developed. Understanding the new mission of universities made it possible to separate the dominants of activities of an innovative and active university (IAU), to develop a scheme of the interconnection of management processes and its basic functions. The authors' interpretation of the IAU and the preconditions for constructing a corporate information and education system (CIES) was formed.

Given the synergism and hybridity of modern cyber threats, the rise of corruption in the educational sphere, the Anti-corruption concept, which provides countering the elements of corruption and integrated hybrid threats through the construction of an adaptive information protection system (AIPS). The basis of corruption counteraction is the digital signature (DS) of the Key Certification Center (KCC) based on PKI (Public Key Infrastructure). To ensure the security of information resources (IR) of CIES, we proposed a model that makes it possible not only to take into consideration the synergy and hybridity of modern threats but also to form preventive anti-corruption measures. A model for providing anti-corruption measures that reflects the scenarios of the behavior of the participants of the corruption process and the anti-corruption bodies was developed. This makes it possible to assess the dynamics of the distribution of corruption deals over time and by the types of corruption to ensure the effective distribution of the university resources for anti-corruption activities

Keywords: innovative and active university, corporate information and education system, model of corruption counteraction

UDC 621.391
DOI: 10.15587/1729-4061.2020.214895

DEVELOPMENT OF METHODOLOGICAL PRINCIPLES FOR THE CONSTRUCTION OF A CORPORATE INFORMATION-EDUCATIONAL SYSTEM OF INNOVATIVE-ACTIVE UNIVERSITY IN THE FRAMEWORK OF ANTI-CORRUPTION ACTIVITIES

S. Yevseiev
Doctor of Technical Sciences, Professor*
E-mail: serhii.yevseiev@hneu.net
O. Rayevnyeva
Doctor of Economic Sciences, Professor, Head of Department
Department of Statistics and Economic Forecasting**
E-mail: olena.raev@m.hneu.edu.ua
V. Ponomarenko
Doctor of Economic Sciences, Professor, Rector**
O. Milov
PhD, Professor*
E-mail: Oleksandr.Milov@hneu.net
Department of Cyber Security and Information Technology
**Simon Kuznets Kharkiv National University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166

Received date 02.09.2020
Accepted date 21.10.2020
Published date 27.10.2020

1. Introduction

The socio-economic transformations of the late 20th and early 21st century are characterized by the processes of progressive globalization and the emergence of a knowledge-based society. This necessitates a change in the paradigm of the functioning of higher education, the search for new approaches, technologies, forms, and methods for organizing the educational process and form the basis of innovative and autonomous activities of universities.

The need to develop an innovative component of higher education is one of the strategic priorities of modernization of the global system of higher education.

Under these conditions, the innovative activity of universities and the formation of autonomous, entrepreneurial universities of the innovative type is one of the forms of integration of the national systems of higher education into the European and world educational and scientific space. At the same time, maintaining their competitiveness and attractiveness is based on the permanent improvement of the quality of education, modernization of its content, implementation of scientific and educational innovations, the introduction of information technologies, and the creation of anti-corruption systems.

In this regard, the study of the characteristics, the dominants of development of an innovative and active university,

development and implementation of information innovations, in particular, the corporate informational and educational system, is an urgent task of management of Ukrainian universities.

2. Literature review and problem statement

The general vector of modernization of the higher education system of Ukraine is the desire to integrate into the European and world educational and scientific space. Since such integration is not possible without systemic reforms, a series of regulations [1–5] that form the legislative framework for empowering universities to choose their own strategies and tactics have been developed over the last decade. On the one hand, these documents create new opportunities for the development of universities, on the other hand, they are sometimes declarative. One of the unresolved problems that universities still face is the poor effectiveness of these acts, as well as the orders of the Ministry of Education and Science, which reflect how they are implemented. Thus, there are difficulties in attracting foreign specialists to teach at public universities, restrictions in the formation of the price of the fee-paying form of education, legal incidents with patents in terms of the distribution of property rights, etc. Therefore, the study and critical analysis of the possibility of implementing the world experience of the functioning of business universities is of particular interest to the management of national universities.

Thus, papers [6–8] show the results of the studies of promising and effective forms, methods of teaching to strengthen the quality of education. It is noted that the creation of the European standards for modernization of higher education brings a positive effect on the reform of national systems. Universities as structural components of the higher education system significantly improve the quality of education, in everyday pedagogical practice implement the idea of a student-oriented approach of teaching and education throughout life. However, the issues of whether all these reforms lead to a change in the paradigm of higher education or they are temporary remain unresolved.

Creation of universities of the innovative type, determining the dominants of their development, the processes of internationalization of universities and economics of knowledge are discussed in [9, 10]. Researchers analyze the challenges faced by innovative and active universities in the process of building new partnerships with business structures and the state. With a university acting as a provider of knowledge to the economy and society in this triad, the problem of how processes within the university can interact remains open. The most controversial among them is how innovative technologies and mixed learning can support teaching people in business; how to adapt the research activities of employees to the challenges of the economy and society.

The study of trends in the development of the higher education system is considered in papers [11, 12]. The authors note that the labor market requires completely new specialists, with new skills and knowledge capable of working in the information society. In this regard, the traditional way of education becomes inadequate for these requests. Universities need not only to change permanently the quality of training specialists but also to do this based on new communication technologies, as well as the models of interaction with students. The main problem that prevents such changes is the readiness of the management of universities and their employees to modernize scientific and educational activities under the new conditions.

The problems of management of the quality in higher educational institutions are explored in papers [13, 14]. The quality of educational services in an innovative and active university is the main source of its competitiveness and attractiveness for applicants and stakeholders. Therefore, the formation and study of the systems of quality, strategies, norms, and systems of values of a university has always been the focus of the university's management. Today, however, a new institutional paradigm of the functioning of quality systems is emerging. In modern systems, an actor-teacher, who affects the entire system of providing educational services of a university by the quality of his labor, is in the center of this system. It is required to explore the problems related to the autonomy of academic staff aimed at improving the personal quality of teaching, developing the motivation systems, and creating effective systems for managing the quality of the scientific and educational activities of employees.

While maintaining the systemic character of the studies by the authors presented above regarding a new understanding of the behavior of an innovative and active university under the fluctuating conditions of the modern stage of civilization development, it should be noted that they did not cover the issues of increasing corruption, of the rapid growth of computing resources, allowing to break into corporate/local networks based on combining cyber threats with the methods of social engineering and synergy with the threats to information security. The issues of constructing a corporate scientific and educational system of a university and the introduction of protocols of global computing systems into the PKI system were proposed in paper [15]. However, the work does not take into consideration the trends of the development of electronic document turnover in modern universities, the construction of e-education, and the tendencies of development of educational services.

The basics of understanding an entrepreneurial, innovative and active university are proposed in paper [16]. Among the key characteristics of such a university are the willingness of universities to adapt to changing conditions and an active search for the ways to adapt in all areas of their activities. With these characteristics, the university seeks to adapt its research, teaching and learning, as well as the ways and forms of knowledge transfer to the current and future needs of the economy and society. It was proved in paper [17] that such changes in the activities of universities depend on the changes that took place in the 21st century in the process of creating knowledge. They are related to the emergence of a distributed system of production and dissemination of knowledge. The author notes that research and learning are no longer an institutional priority only for universities, but rather a broad interaction with the surrounding society, its diverse stakeholders, based on the involvement of modern information and communication technologies in this process. A modern university is one of many structures involved in the production of knowledge, and the problem is not only the need to improve the software of the courses taught. The main task of an innovative and active university, which requires further research, is to become a leader in training intellectual workers, to find effective methods and ways to make a university attractive in the competitive educational space.

Paper [18] proposes a taxonomy of corruption in higher educational establishments that helps detect, categorize, and analyze corruption. This classification helps understand the causes and consequences of corruption, as well as to identify situations in universities, with the occurrence of which the probability of corruption at all levels increases. For example, stakeholders and anti-corruption practices will be different in situations of administrative corruption compared to bribery cases initiated by teachers. However, this work does not take into consideration the dynamics of corruption processes, accounting of which would help to identify the ways of formation and development, as well as the ways of blocking corruption processes. These shortcomings are common for most works on corruption at universities.

Study [19] provides an overview of the literature on the classification of corruption mechanisms. Corruption is said to occur at the level of the Ministry of Education, regions/districts, universities, or educational institutions. Determining the level of occurrence helps to identify participants involved in corruption schemes in order to apply legal measures to prevent their activities. However, the preventive anti-corruption measures under consideration have a limited scope of application, which is determined by a specific current situation, and further research is needed to give universality to anti-corruption measures.

The conducted analysis [20–25] showed that corrupt actions in the field of education imply any actions that violate the normal/standard regulation and development of a university in order to pursue personal or corporate interests at the expense of public interest.

The main types of corruption in education and their causes are shown in Fig. 1.

Analysis of Fig. 1 showed that the peculiarity of the formation of mechanisms of anti-corruption public administration of higher education institutions under conditions of European integration and innovative development is:

– narrowing the functions of the direct impact of the state on the educational sphere;

– improvement of the legal status of higher educational establishments;

– introduction of modern organizational and financial maintenance in the state management of institutions [26].

At the same time, the most common schemes of corruption are:

– entrance examination to a university;

– corruption activity related to getting high marks throughout the entire university career;

– corruption at the final stage of doctoral studies;

– corruption at the administrative level [27].

Anti-corruption activities in education are implemented through general organizational and legal measures. However, the specifics of this area necessitate the development and realization of additional anti-corruption mechanisms that take into consideration the industry specifics. The key factor of existence or the absence of the corruption component is the quality of higher management.

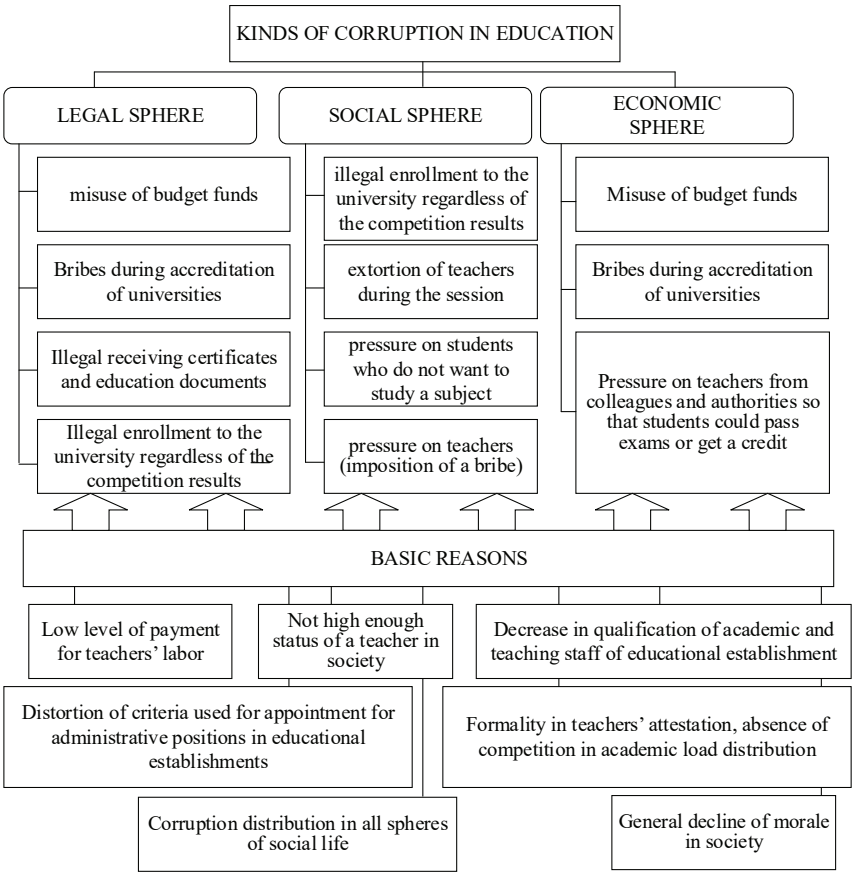

Fig. 1. Relationship between the main types of corruption and their causes in education

Thus, detection and displaying of corruption, first of all, requires a structure (taxonomy) [28] that allows identification of the types of corruption that have become known. Secondly, to assess the corruption hierarchy, it is necessary to use the structure presented in research [28]. Finally, the "fraud triangle" model examines the stimulation structures for the involvement in corruption activities that need to be taken into consideration to provide policy recommendations to combat corruption at modern universities [29]. However, this approach does not take into consideration the potential of IT-technologies to combat modern types of corruption in the educational sphere.

3. The aim and objectives of the study

The aim of this study is to develop methodological principles for the construction of a corporate informational and educational system (CIES) of an innovative and active university as an anti-corruption tool.

To achieve the set goal, the following tasks need to be solved:

– to explore the modern paradigm, dominants, and functions of an innovative and active university;

– to substantiate the criteria for selecting methodological principles for constructing an innovative and active university in an anti-corruption environment;

– to develop an anti-corruption model and carry out the simulation.

4. Exploring the modern paradigm, dominants, and functions of an innovative and active university

Universities are currently facing serious competition from institutions that provide online education and training services.

The reason for the emergence of such institutions is usually the lack of effective interaction between universities and companies-employers, consumers of professionals with higher education. As a result, there is a persistent myth about certain obsolescence of competencies, obtained in universities, from the needs of real sectors of the economy, public administration, and society.

All this causes the need for universities to adapt to new conditions, and, as noted in [30], need to change the structure of university DNA from within based on permanent innovations.

In fact, the processes that are characteristic of the modern stage of higher education development in the world are tolerant of entrepreneurial processes, where any competing firm or organization is looking for effective strategies, ways, tools to gain a competitive advantage.

An in-depth study of the sources of competitiveness in entrepreneurship at the beginning of the 20th century has identified innovations as a key factor.

Thus, the innovative and active work of any organization is defined as the creation, search for, and using the opportunities for the new ways of doing things that lead to the improvement of the systems and ways of managing people and organizations.

While the specifics of innovative activities are well studied for business structures, the entrepreneurial and innovative activities of universities are a phenomenon of the late 20th and early 21st centuries. Its emergence is directly related to the processes of globalization, the autonomy of universities' activity against the background of reduced public funding for their activities. This, in turn, transforms once state economic entities into entrepreneurial structures, changing the approaches, methods, and types of their activities.

In addition, the evolution of the activities of universities, manifested primarily in the evolution of the mission of their activities, is directly related to the industrial revolutions (Fig. 2).

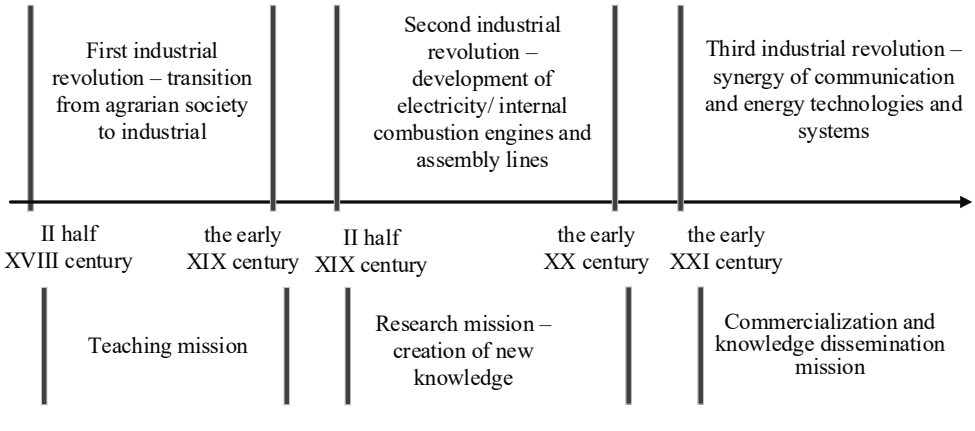

Fig. 2. The evolution of industrial revolutions and university missions

The analysis of these works [30 40] allowed forming an evolutionary model of spirals, which includes the main stakeholders of the interaction of universities (Fig. 3), namely:

– a simple spiral, corresponding to the teaching mission of universities.

The main purpose of universities' activities is to accumulate, preserve and transmit knowledge;

– the double spiral originated from the interaction of universities with industry and transformed the university's teaching mission into research by adding a function of generation/creation of new knowledge. Academic and industry-related interactions became the basis of joint innovations and created the prerequisites for the formation of an entrepreneurial university. However, the main activity of universities remains educational activity;

– the triple spiral of interactions reflects a new view of a university, its academic system, which is based on new models of cooperation between industry consortia, university relations, and government agencies. There appears an entrepreneurial university, the distinctive characteristic of which is the versatility and interconnectedness of its activities based on a variety of innovations. Under these circumstances, its mission is not only to create new knowledge, but also to commercialize and disseminate it in scientific, industrial, and social circles;

– the quadruple spiral is a modification of the triple spiral and supports its mission. The fourth player in the relationship is civil society, which supports a democratic approach to innovation, the essence of which is the social responsibility of politics and practices to create and implement innovations for future generations.

Based on the knowledge theory [41], it is known that innovations:

– firstly, need knowledge that is distributed among a large number of different innovative and active participants;

– secondly, include latent, human-embodied knowledge, which is not always easy to convey.

That is, the innovation process is an iterative process of the emergence of new knowledge from the existing ones in new forms. Of all the subprocesses of cognition, namely, creation, exchange, acquisition, transfer, and application of knowledge, the creation of knowledge has a dominant influence on innovation [45]. Consequently, among the quadruple spiral of interactions, universities play a key role, and adaptation to the task of creating entrepreneurial thinking, stimulating setting up businesses, and using the ideas in society is the key to their survival.

Thus, at the beginning of the twenty-first century, a new paradigm for the development of entrepreneurial universities, which implies that universities are called upon to serve society by supporting the economy and improving the quality of life of their citizens, was formed [46].

The new paradigm fundamentally changes the culture of responsibility and the value system of a university as evidenced by the spread of managerial

approach and the use of the principle of value for money in higher education systems around the world. Competitiveness and relevance of the university's existence are assessed mainly in accordance with its contribution to the economic development of countries and humanity as a whole. To adapt to the new paradigm, some adaptation is required – the adaptation of the university's relations with the surrounding society/core stakeholders, the adaptation of its internal processes, core values, and finding new innovative foundations for its development in today's environment. Fig. 4 shows the relationship between management processes and the main functions of an innovative and active university, taking into consideration the development of e-education.

Currently, there are two different approaches to understanding the essence of an entrepreneurial, innovative, and active university.

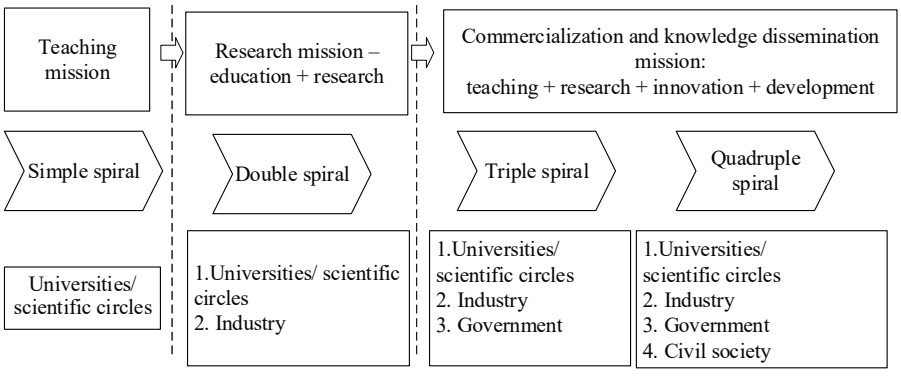

Fig. 3. An evolutionary model of the spirals of university's interactions with the economy and society

The first approach treats it as an institution that does its best to develop science, invent new technologies, and stimulate new markets and industries. At the same time, the entrepreneurial aspect of the activities of universities is associated exclusively with business and the commercialization of their intellectual property.

This view is largely supported by the views of the international community (for example, organization of economic cooperation and development (OECD), which considers universities as sources of technological innovations and "growth engines". At the same time, the criteria for the innovativeness of the university are the number of submitted national and international patents, their citations in the development of new patents, the influence of patents, etc. A variety of ratings are based on these criteria, in particular, the Reuters agency rating, which was compiled in cooperation with Clarivate Analytics "Top 100 most innovative universities in the world" [47]. By results of 2019, for the fifth year in a row, three universities have had the leading positions in this direction – Stanford University, the Massachusetts Institute of Technology and Harvard University. The list of the countries with the largest number of innovative universities in the top 100 includes the United States (46 universities), Germany (9), France (8), United Kingdom (6), South Korea (6), and Japan (6).

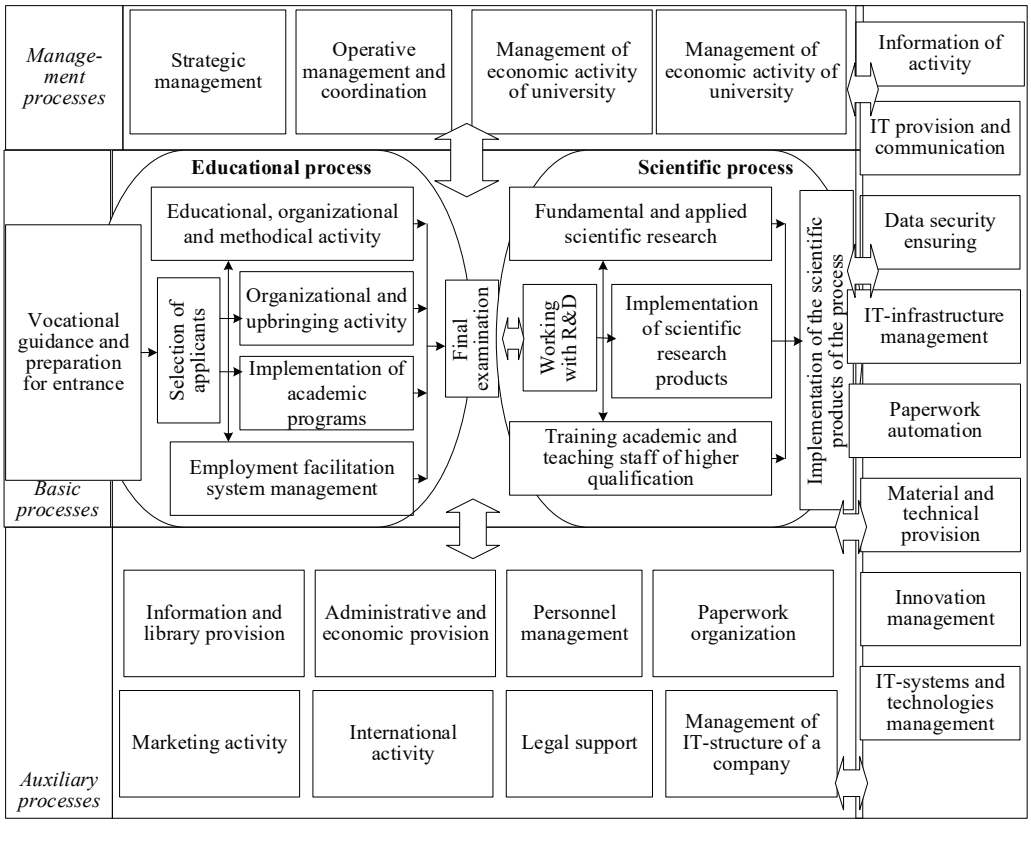

Fig. 4. Scheme of the interconnection of management processes and the main functions of an innovative and active university

The second approach considers more widely the innovative and active work of a university. It defines it as a totality of new initiatives in the leadership organization and development; experiments in pedagogy, knowledge organization, the introduction of new forms of education and development of academic programs that are relevant to the requirements of business and society. Interaction between internal and external stakeholders plays a special role in the approach; interdisciplinary scientific activities related to obtaining new knowledge, methods, and commercialization of their results.

This approach is related to the concept of entrepreneurship, which focuses on two key objectives: formation of an enterprising person and development of entrepreneurial thinking [46, 48–51].

Supporting the imperatives of the second approach, the article proposes the authors' understanding of the IAU. The IAU implies an entrepreneurial organization that has resource readiness to contribute to accelerated socio-economic development through the intensive transfer of knowledge and technologies generated at the university based on partnership with stakeholders. At the same time, the latter includes labor market actors, governmental and public organizations.

In this context, the dominants of the IAU activities are:

– science as a tool to generate new knowledge based on the integration with the external environment, especially with high-tech enterprises;

– education as a way of bringing knowledge to people, the formation of the intellectual potential of the society;

– interaction with industry, government, society as a means of concerted efforts to ensure the stable development of the nation and civilization.

Fig. 5 proposed an operating model of the university's interaction with stakeholders.

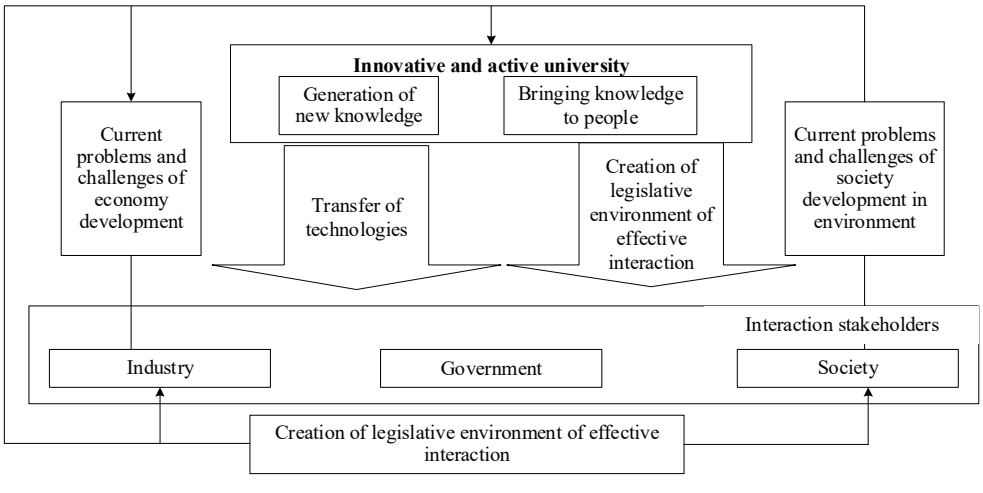

Fig. 5. The operational model of the university's interaction with stakeholders

Modern information systems and technologies are the platforms for maintaining effective interaction between a university and stakeholders. Therefore, an integral part of the IAU management is the system of corporate management of the provision of educational services, which, based on the use of modern software, creates effective electronic document turnover and acts as a tool to prevent corruption at the university.

In addition, in the context of increasing aggressiveness of the external information environment and modern hybrid threats, there appears the need to ensure the security of information resources of the CIES and the creation of models to maintain the safe contour of the main business processes of a university.

Thus, the proposed approach provides objective control on the part of society over the academic activities of educational institutions, which contributes not only to the quality of the formation of basic education services but also to the formation of competitive qualities of students.

5. Choice of criteria for the construction of methodological principles for the formation of the CIES of an innovative and active university in an anti-corruption environment

The basic component of the proposed methodology is a corporate informational and educational system based on the Open Systems Interconnection Basic Reference Model, which uses open protocols to ensure the security of CIES information resources.

The studies conducted in paper [54] showed that virtually all protocols are open-ended, which significantly reduces the ability to provide security (security services) at all levels of the ISO/OSI mode. Table 1 gives the main protocols to ensure circulation and processing of the IR of the CIES.

However, the studies carried out in paper [55–57] show the need to tighten security requirements based on web technologies and the use of commercial solutions to construct the AIPS.

To ensure preventive measures against the manifestation of corruption elements through the introduction of electronic turnover and elements of e-education in modern educational institutions, it is proposed to use the PKI technologies, based on the digital signature (DS) that relies on standard X.509.

The use of a cryptographically resistant mechanism based on the digital signature (DS) mechanism makes it possible to ensure the formation of the Concept of security and corruption counteraction in educational institutions. In this case, the concept should be seen as a methodological basis for security at various management levels, the hierarchy of which was proposed based on [58].

The functioning safety of an innovative university is implemented at the following levels:

– at *the strategic level* – university authorities – the creation of conditions for the impossibility of making corruption changes in the guidelines on the organization of the educational process, providing basic public and communication services of the university's activities, conditions of students' life and transparency of rendering educational services. Ensuring effective control of keeping to the academic schedule at the university's faculties;

– at *the operational level* – faculty authorities, departments, and services involved in the system of service

delivery – prevention of corrupt changes in the objectivity of students' assessment in the process of learning, accruing scholarships (grants, etc.). Organizing exams throughout the entire cycle of the educational process, creating conditions for effective monitoring of the implementation of the academic schedule for the specialities of a faculty, preventing corruption in departments and services of a university;

– at *the tactical level* – heads of departments – rising the level of objectivity of students' assessment in certain disciplines, creating the conditions of transparent students' choice of academic disciplines from the unit of an elective component of the educational process. Creating conditions for effective monitoring of the implementation of the academic schedule by teachers of departments.

Table 1

Basic protocols for ensuring circulation and processing the IR of CIES

Level	Information	Protocols
Applied: access to network services	Data	HTTP, gopher, Telnet, DNS, DHCP, SMTP, SNMP, CMIP, FTP, TFTP, SSH, IRC, AIM, NFS, NNTP, NTP, SNTP, XMPP, FTAM, APPC, X.400, X.500, AFP, LDAP, SIP, IETF, RTP, RTCP, ITMS
Representation: data representation and encoding	Data	IMAP, POP3, SMB, MFTP, BitTorrent, e2k, PROFIBUS and many other
Session: connection session management	Data	ASN.1, XML, TDI, XDR, NCP, AFP, ASCII, Unicode
Transport: safe and reliable connection «point – point»	Units	ASP, ADSP, DLC, Named Pipes, NBT, NetBIOS, NWLink, Printer Access Protocol, Zone Information Protocol, SSL, TLS, SOCKS, PPTP
Network: determining the route and IR (logical addressing)	Packets	TCP, UDP, NetBEUI, AEP, ATP, IL, NBP, RTMP, SMB, SPX, SCTP, DCCP, RTP, STP, TFTP
Channel: MAC and LLC (physical addressing)	Frames	IPv4, IPv6, ICMP, IGMP, IPX, NWLink, NetBEUI, DDP, IPSec, ARP, SKIP
Physical: cable, signals, binary transmission	Bites	ARCnet, ATM, DTM, SLIP, SMDS, Ethernet, FDDI, Frame Relay, LocalTalk, Token Ring, PPP, PPPoE, StarLan, WiFi, PPTP, L2F, L2TP, PROFIBUS

The concept of security and corruption counteraction is presented in Fig. 6, *a–c*.

The first level describes the overall corporate strategy of a university and its functional strategies in ensuring the security of confidential (personal) data while providing educational services to students. At this level, according to the synergistic approach, the overall concept of ensuring CIES security is considered and the aims and objectives of cybersecurity are formed. Functional strategies of one level have horizontal connections and are aligned at the goal level, followed by detailing at the next level of the strategic set.

At the second level, the corporate strategy and information security in the CIES is formed, the goals and objectives of the main business processes related to the protection of personal data of the university's legal and physical partners in the provision of educational services are determined.

At the third level, an adaptive system for protecting the information resources of the CIES is formed based on modern security mechanisms. It is recommended to use commercial cryptographic systems to prevent crypto-bookmarks.

The proposed approach takes into consideration not only the basic functions of the hierarchical structure of the IAU management, their aims and objectives, but also the counter-response to the elements of corruption and integrated hybrid threats based on the construction of the AIPS.

The main elements of the AIPS are the KCC, which provides not only authentication/authorization but also automatic control of electronic document turnover, which greatly reduces the risks of corruption schemes at all levels of the IAU management.

In addition, the LDAP server, which is a part of the KCC, allows ensuring the safe authorization/authentication of CIES users.

This approach provides the DP services to state authorities, local governments, businesses, institutions, and organizations of any form of property, as well as physical entities. Fig. 7 shows a physical virtual network for the deployment of a system of comprehensive information protection (SCIP) based on the PKI infrastructure [52, 53].

To verify a DS, a key certificate is used – an electronic document issued by the certifying center (CC) or by a trustee of the CC and confirming that the DS verification key belongs to the holder of the DS certificate [52, 53].

Fig. 8 shows the variant of the block diagram of CIES of an information active university, taking into consideration the basic functions of information resource management and security (IR IIAS) in the face of hybrid threats and possible corruption schemes. As a rule, CIES is formed based on web technologies that make it possible to meet the requirements of informativeness, openness, and accessibility to IR of CIES.

Therefore, in addition to ensuring the authenticity of the KCC-based IR of CIES, it is proposed to use commercial implementation of the crypto-code designs by McEliece and Niederreiter to ensure IR confidentiality and integrity. This approach will ensure not only the required level of crypto resistance under conditions of the emergence of a full-scale quantum computer, the speed of crypto-transformations at the level of block-symmetrical ciphers, reliability, but also counteraction to cyber bookmarks based on encryption standards [59]. The basics of practical construction of crypto-code designs by McEliece and Niederreiter on modified elliptical codes and flawed codes are considered in papers [60–63].

Thus, the proposed approach to providing basic security services makes it possible to ensure the required level of security of the IR of CIES and to counteract modern cyber threats, both external and internal.

The conceptual synergistic security model of CIES (corporate information and educational system) of the IAU is based on particular models: advanced models of the CIES infrastructure and of an attacker, a synergistic threat model that makes it possible to assess security level.

The improved model of the CIES infrastructure is described by the model:

$$G^{CIES}=\{\{O^{CIES}\},\{L^{CIES}\},\{I_A\}\}, \quad (1)$$

where $\{O^{CIES}\}$ is the set of environment objects describing the elements of the KIO infrastructure and their belonging to the levels of ISO/OSI model, $\{L^{CIES}\}$ is the set of relations between the elements of the infrastructure, determined by the adjacency matrix

$$A^{CIES} = \left\| a_{ij}^{CIES} \right\|.$$

$\{I_A\}$ is the set of elements of information assets. Each element $I_{A_i} \in \{I_A\}$ is described by vector $I_{A_i} = (Type, A^C, A^I, A^A, A^{Av})$. Type is the type of information assets, described by the set of basic values $Type=\{PlD, StO, OI, YI, PD, SI\}$, where PlD is the payment documents, StO is the statistic reports, Ol is the public information, YI is the management (regulatory information), PD is the personal data of CIES users, SI is the scientific information (know-how).

A^C is privacy, A^I is integrity, A^A is authenticity, accessibility, A^A is continuity – the information properties to ensure. They accept the value of 1 if a property is necessary, 0 – otherwise.

Each element $O_l \in \{O^{CIES}\}$, is described by vector $O_l = \{Y^{CIES}, IO\}$, where Y^{CIES} is the level of information structure hierarchy, determined by set $Y^{CIES}=\{FL, NL, OSL, DBL, BL\}$, where FL is the physical level, NL is the network level, OSL is the level of operation systems (OS), DBL is the database management level, BL is the level of technical applications and servers. The following rule is used to indicate the type of connection and existing relation IO^R between information assets and environment objects:

$$IO^R = \left\| IO_{il}^R \right\|, \quad (2)$$

where IO_{il}^R displays the existence and the type of relations between the i-th information asset and the l-th environment object. In this case $\forall i \in \{I_A\}$, and $\forall l \in \{O^{CIES}\}$:

$$IO_{il}^R = \begin{cases} 0, \text{ no connection;} \\ cs, \text{ includes and stores;} \\ pt, \text{ processes and transfers;} \\ so, \text{ maintains functioning.} \end{cases}$$

The synergistic model of threats can be formally presented as:

$$ThM_{syn}^{CIES} = \begin{Bmatrix} \{DF^{CIES}\}, \{T_{risk}\}, \\ \{T_P\}, \{T_U\}, \{VH\} \end{Bmatrix}. \quad (3)$$

The set of the sources of CIES safety threats is represented by the tuple $DF^{SIES} = \{V^{NS}, V^{AS}\}$, in which V^{NS} is the class of natural threat sources, $V^{AS} = \{V^{ACS}, V^{AIS}, V^{ASI}\}$ is the class of anthropogenic threats, where V^{ACS} is the set of threats to cyber safety, V^{AIS} is the set of threats to information security, V^{ASI} is the set of threats to the safety of information. T_{risk} is the qualitative risk indicator, T_p is the set of basic terms of probability of implementation of at least one threat to the j-th asset, T_U is the set of basic terms of the magnitude of damage from the implementation of threat u_i, VH is the set of destructive states of the elements of the CIES infrastructure, which imply an undesirable and unplanned state of the CIES element, in which it got as a result of the implementation of one or several threats.

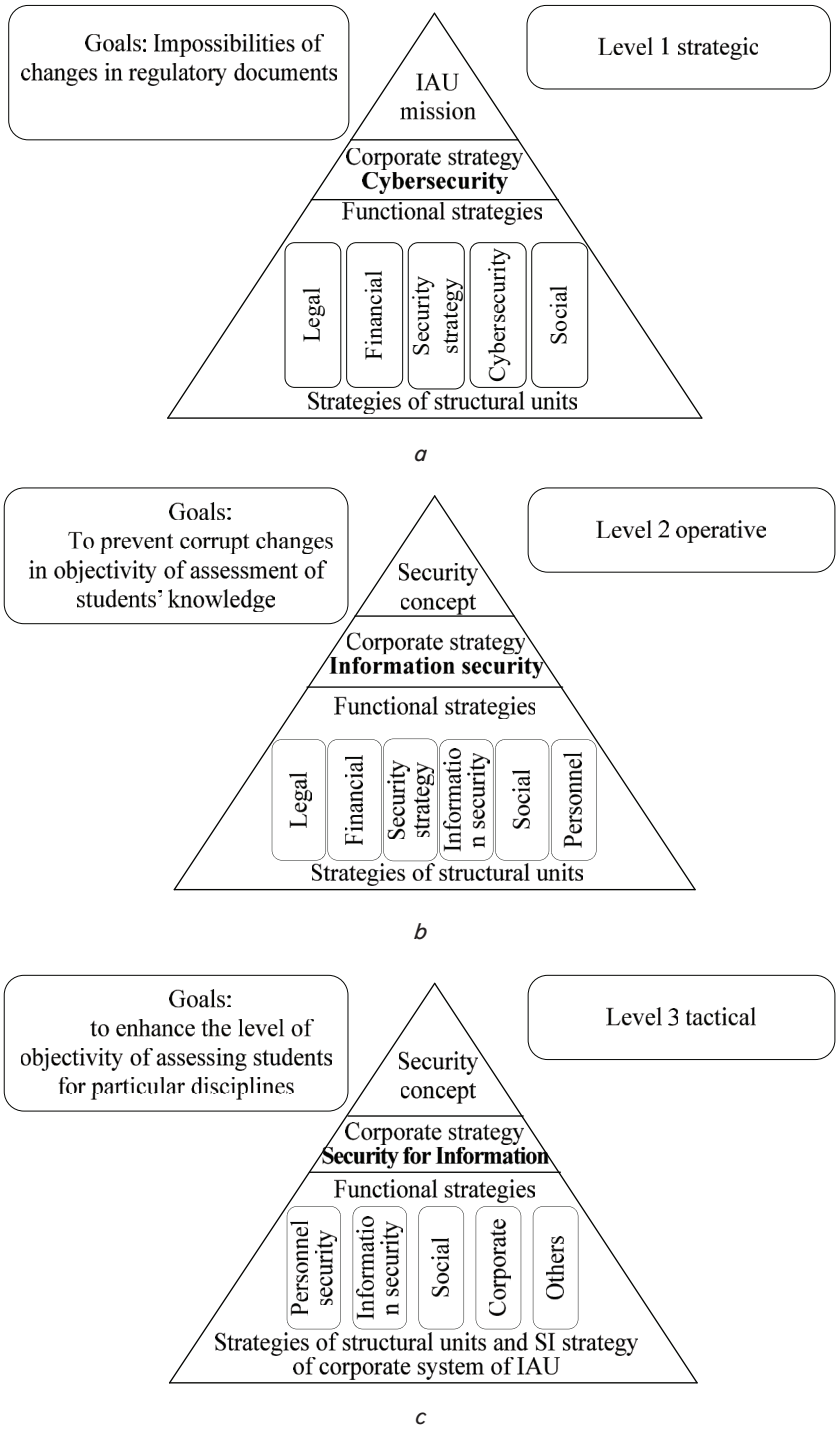

Fig. 6. Concept of corruption counteraction: *a* — strategic level; *b* — operational level; *c* — tactical level

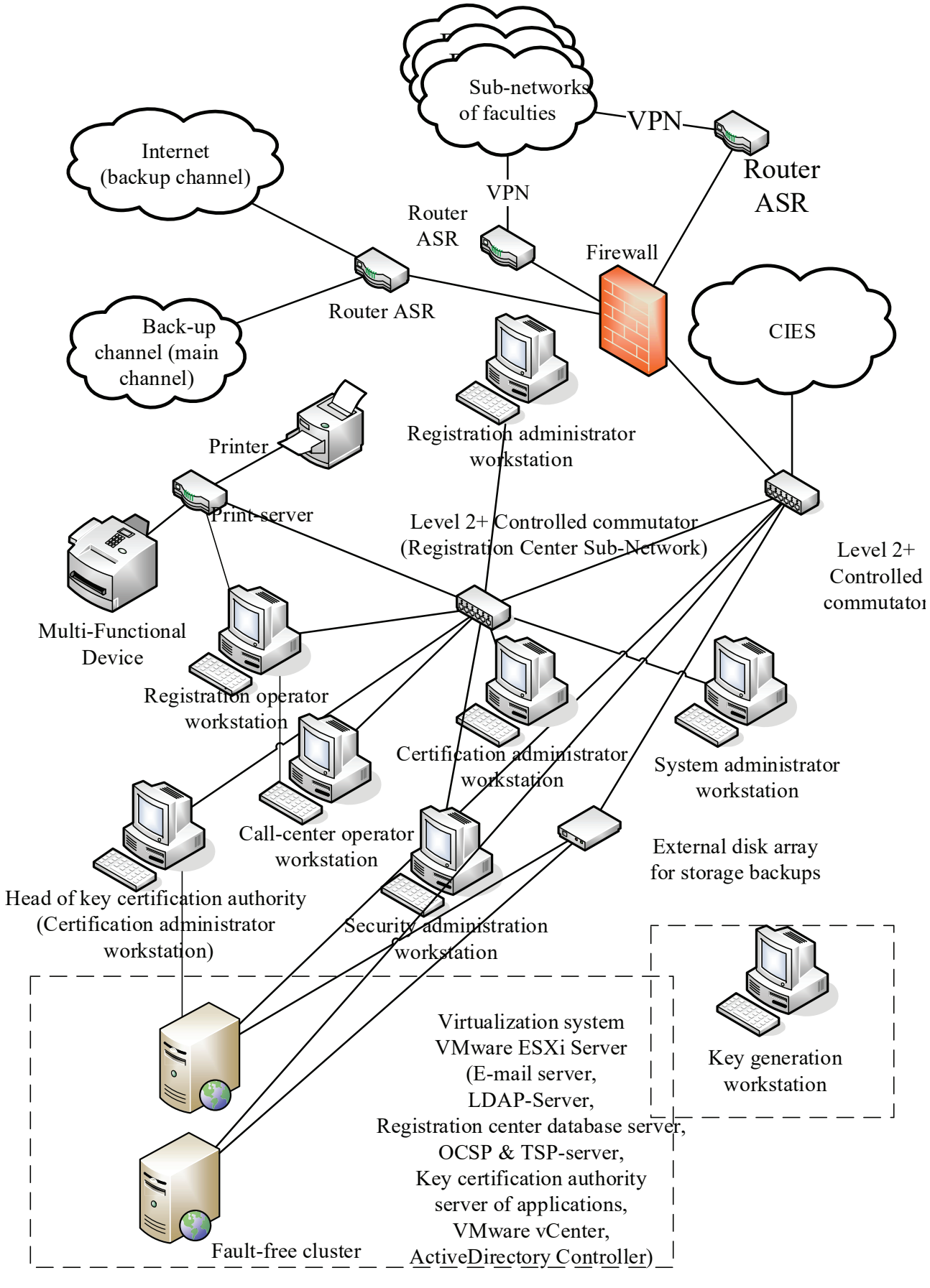

Fig. 7. The physical network of the PKI infrastructure

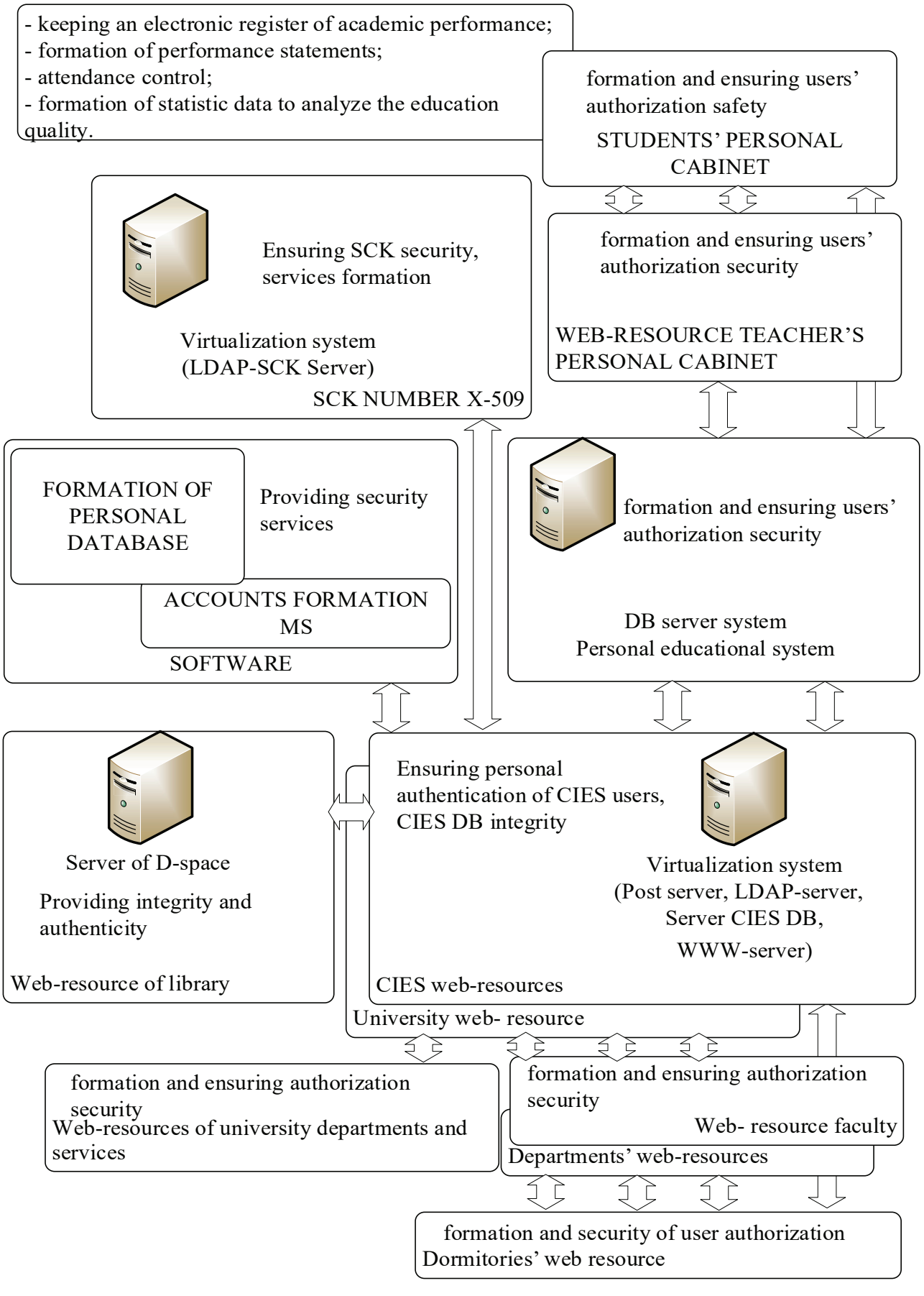

Fig. 8. A variant of the block diagram of CIES of an innovative and active university

In order to have a synergistic effect of increasing the information security level, it is necessary to take into account the complexing of threats:

$$DF^{CIES}=\{V^{NS}\}\cup\{V^{AS}\},$$

where

$$\{V^{AS}\}=\{V^{ACS}\}\cap\{V^{AIS}\}\cap\{V^{ASI}\}, \quad (4)$$

where each element of the set of threats $DF_i\in\{DF^{CIES}\}$ can be represented by the following vector of values of DF_i (T, T_p, pr_{ij}, r_{motiv}), where T is the time of successful implementation of a threat, T_p is the set of basic terms of probability of implementation of at least one threat to the j-th asset, pr_{ij} is the probability of implementation of at least one threat to the j-th asset, i is the threat, $\forall i\in n$, n is the number of threats, j is the information resource (asset), $\forall j\in m$, m is the number of assets; r_{motiv} is the probability of attacker's motivation to implement a threat.

However, the estimate of the probability of implementation of the i-th threat to the j-th asset will be determined taking into account the relations between the threat sources and CIES elements, which is assigned by matrix $A^{DF}=\|a_{ij}^{DF}\|$, dimensionality n on m, where n is the number of threats, m is the number of assets. For each i-th threat to the j-th asset, we determine the probability of implementation of pr_{ij} based on accumulated statistic data, characteristic of the given region and operation conditions (in the quantitative and/or qualitative form) or in an expert way.

The probability of the implementation of at least one threat to each asset is calculated according to the following formula:

$$p_{rj}=1-\prod_{i=1}^{m}(1-pr_{ij}), \quad (5)$$

where p_{rj} is the probability of implementation of at least one threat to the j-th asset.

It is supposed that in case of implementation of at least one threat from set $V^{AS}=\{V^{ACS},V^{AIS},V^{ASI}\}$ to the j-th asset, the damage is equal to the cost of the asset based on detailing the assets and through the selection of actual threats:

$$q_j=u_j. \quad (6)$$

It is believed that threats can be implemented independently of each other, then the price of risk R_j for each j-th asset is determined from the following formula:

$$R_j=pr_{ij}\times q_j. \quad (7)$$

The full cost of risk is equal to the sum of costs of risk of all assets:

$$R_{full}=\sum_{j=1}^{n}R_j. \quad (8)$$

Thus, the probability of implementation of environment p_{rj} with the region of determining P=[0, 1] will be assigned by the set of basic terms T_p={non-implemented, minimum, medium, high, critical}={α_{x1}, α_{x2}, α_{x3}, α_{x4}, α_{x5}}.

The formal improved model of an attacker will be determined taking into consideration the proposals in papers [52, 62], in which the categories and actions of attackers are determined as:

$$G_{IA}^{CIES}=\{aid_i,T_{IA},S_{\max_i},pr_{ij},r_{motiv}\},\ \forall i\in n,\ \forall j\in m, \quad (9)$$

where $aid_i\in\{aid\}$ is the attacker's identifier, T_{IA} is the time of successful implementation of a threat, $S_{\max_i}$ is the probabilistic damage of a system, pr_{ij} is the probability of implementation of at least one threat to the j-th asset, i is the threat, $\forall i\in n$, n is the number of threats, j is the information resource (asset), $\forall j\in m$, m is the number of assets; r_{motiv} is the probability of motivation of an attacker to implement a threat.

To assess threats, we use a set of sources of threats, which include the sources of four types:

$$DF^{CIES}=\{V^{NS},V^{AS},TS,PI,NI\}, \quad (10)$$

where TS is the technical means and systems; PI is the deliberate attackers; NI is the non-deliberate attackers (offenders).

Thus, the proposed model makes it possible to take into consideration the complexing of threats, their synergy and hybridity, to form preventive measures based on the analysis of crucial threats and critical points in the CIES infrastructure.

6. Development of the model of corruption counteraction and simulation

Corruption refers to any actions that violate the standard regulation and development of any activity sphere by using public opportunities to pursue personal or corporate interests at the expense of public interests [18–20].

Thus, corruption in education will mean the activities of people authorized to perform the functions of the state, aimed at the illegal use of the powers granted to them to obtain material goods, services, benefits and other advantages. In this case, interests are not necessarily material, they may be intangible when actions are made in accordance with some ideas or for ideological reasons.

Scenarios of the behavior of corruption process participants and anti-corruption bodies can be represented as a mathematical model.

The target of the model of the behavior of various participants of corrupt actions is, first of all, the possibility of scenario simulation of the behavior of parties. This ultimately influences the choice of the direction of anti-corruption action and investment of limited funds in anti-corruption programs.

To achieve this goal, the following tasks need to be addressed:

– to identify the basic concepts used in models of behavior of participants in corruption actions that directly influence the decision to direct the tools to prevent and protect against corruption, as well as assumptions and limitations of the model;

– to develop mathematical models of behavior of the conflict parties that influence decision-making or a change of earlier made decisions to prevent corruption;

– to perform simulation based on the developed mathematical model to prove the logic of behavior of conflict parties and assess the impact of their behavior on the use of the anti-corruption budget.

The conducted analysis enabled the formation of a list of basic concepts and notions used in describing processes in corruption prevention systems, which should be used in the developed model of the behavior of participants' corruption actions. Table 2 shows the basic notions of financial strategies in the corruption prevention systems, which are the basis

for the interaction of participants in the corruption process in a dynamic model of behavior.

The generated concepts are incorporated into the mathematical model because they reflect the nature of the interaction between participants in a corruption process and influence the distribution of limited anti-corruption tools.

The model of the behavior of the conflict parties is based on the assumptions and limitations shown in Fig. 9.

The model does not include various financial indicators and approaches, such as: cost-benefit analysis, risk analysis, net present value (NPV), annual estimation of corruption-related losses (ALE), etc. These issues may be considered as the areas of future research.

The model focuses on the dynamics of interaction between participants in the corruption process to identify the strategies used in the anti-corruption process.

It describes the behavior of the anti-corruption party, which is trying to oppose the implementation of a corrupt operation that could have an impact on the university's reputation, ultimately resulting in financial losses.

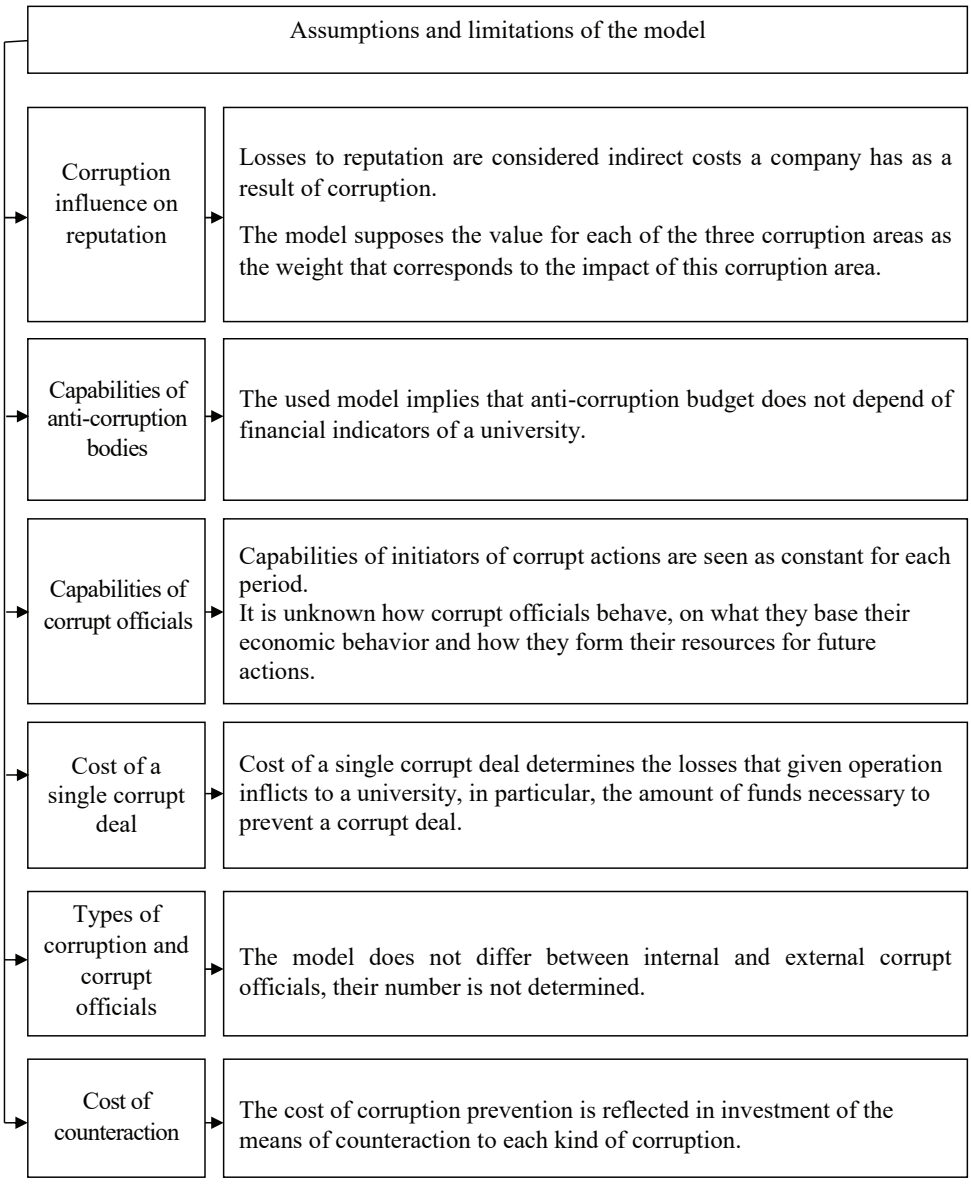

Fig. 9. Assumptions and limitations of the model of the behavior of conflict parties

Table 2

Key concepts in the models of behavior of corruption participants

Concept	Definition
Reputation (*Rep*)	An authoritative and universally recognized name or position for merits, achievements, reliability, and the like. In this case, the reputation belongs to the public prestige of a university
Vulnerability (*Vul*)	The level of reliability of the university's anti-corruption system
Security vectors (V_i)	Corruption types are outwardly visible and accessible university resources that can be used to carry out corrupt transactions and subsequently assessed according to the potential harm that could be caused to the reputation of a university
Capabilities of an anti-corruption party (C^D)	Available resources to be distributed to improve the level of protection of the university's assets from corrupt transactions
Capabilities of corruption initiators (C^A)	Part of the resources of corrupt officials available for distribution among the university staff
Fraction of investment (*FI*)	Part of the university's capabilities, meant to protect the university's assets from corrupt transactions
Fraction of corrupt deals (AF^i)	The number of corrupt deals that corrupt officials make in accordance with the types of corruption.
Successful corruption deals $\left(A_i^S\right)$	Acts of corruption that have achieved the goal and brought the expected result
Profit of anti-corruption system (*DAP*)	Monetary profit from the implementation of counteraction to corrupt deals, which in turn enhances the reputation of a university, increasing its financial indicators
Profit of corrupt officials (C^A)	Monetary advantage gained as a result of performed corrupt deals

The formation of the model is limited to three possible areas of corruption – the admission committee (type 1 corruption), current educational activities (type 2 corruption), and administrative activities (type 3 corruption). Counteraction to corruption must be implemented in each direction. Anti-corruption measures are considered effective if the corresponding corruption operations are prevented or detected.

The model consists of three sub-models – the sub-model of a corrupt official, the sub-model of the environment of corruption implementation, and the sub-model of the anti-corruption parties, the connection between which is shown in Fig. 10.

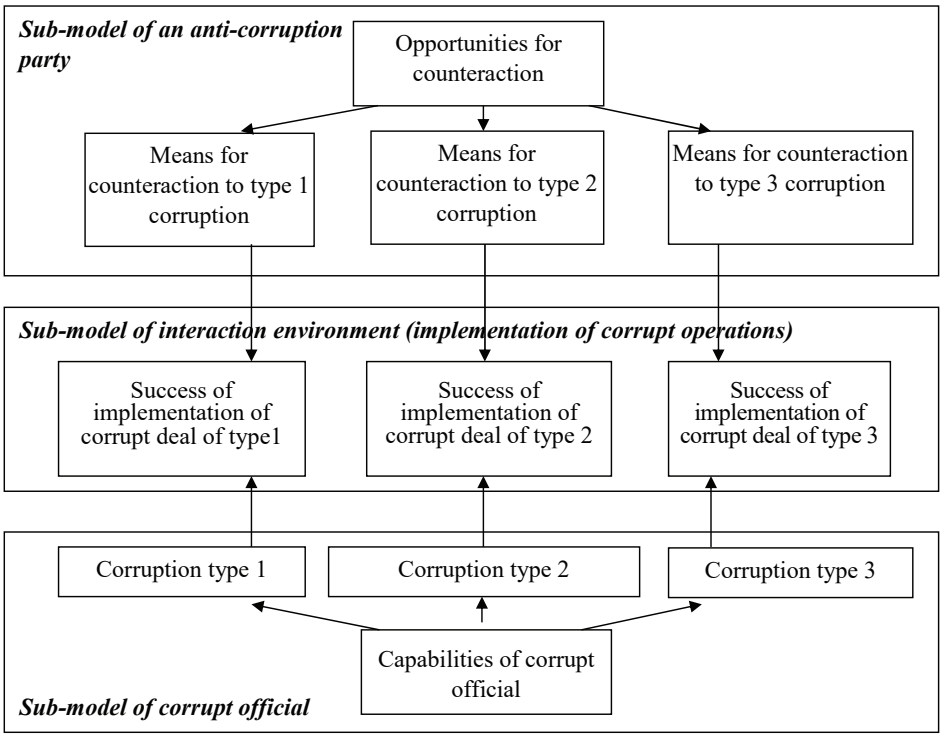

Fig. 10. The general structure of the anti-corruption model

The anti-corruption model represents a mechanism for corruption prevention or detection. In each period, the anti-corruption party decides whether to channel the available funds to prevent corruption. It is assumed that the opposing party has the necessary means of influencing each type of corruption, and their capacity is sufficient for additional efforts, which are necessary in the event of a threat to the reputation of a university in the event of corruption.

The anti-corruption party organizes the prevention (or detection) of corrupt deals through countermeasures, which are displayed by the units of success of corrupt deals. The counteraction result ultimately affects the reputation of a university, which can be evaluated by financial results. The unit of success of the implementation of a corrupt deal is determined by the probability that this deal will be successfully carried out and not disclosed in the future. For each unit, the success of anti-corruption actions is counted. The direction of funds to counteract corruption of one type or another is calculated based on the share of successful anti-corruption actions on a particular type of corruption.

The reputation of a university is estimated in relative units. It is adjusted by the results of identified or prevented corruption deals for all corruption types. In the case of successful corruption counteraction, the reputation of a university increases, while successful corruption deals lead to the loss of reputation.

The financial indicators of a university are determined based on expert estimates of monetary expression of each reputation point.

A corrupt official is focused on making a corrupt deal and makes some efforts to do so.

It should be noted that the same person may be interested in making various types of corrupt deals. However, its focus on some form of corruption is mostly fixed for a specific period.

He can base his actions on information received both from official sources and informally transmitted information. It should also be taken into consideration that a corrupt official will attempt to implement corrupt deals that will bring him greater profit (direct or indirect) than the funds spent on the implementation of such an operation.

The efficiency of a corrupt official can be determined as the sum of all successful corrupt deals multiplied by the profit derived from the corresponding deal.

To display the interaction between corrupt officials and the anti-corruption parties, each of which has certain capabilities and makes appropriate decisions, the third sub-model – the sub-model of the interaction environment – was implemented. The main variables of this model are the probability of successful corruption deals of each corruption type. These probabilities are determined, in turn, by the level of efficiency of anti-corruption measures for a particular type of corruption. The high values of probability of a particular corruption type indicate weaknesses in providing counteraction to the given type.

The main ratios between the previously described variables determine the essence of the relationship between the participants in the counteraction process, leading to a change in the investment scenario and redistribution of the university's funds for anti-corruption activities. The formal representation of these ratios is shown below in the form of a system of algebraic and differential equations.

Given the existence of feedback (amplifying and damping contours) in the actual interaction of the parties of the anti-corruption process, it would be appropriate to indicate the moment for each variable, but such a record would make the equation system much more complicated.

The main ratios for each sub-model are:

– sub-model of the counteraction party:

$$A_i^{RS}(t)-A_i^{RS}(t-1)=(R_i-D_i)\Delta t,\quad R_i=A_i^S/T^{RA},$$

$$FI_i=A_i^{RS}/\sum_{i=1}^{3}A_i^{RS},\quad \frac{\mathrm{d}(Rep)}{\mathrm{d}t}=BU-ER,$$

$$BU=\begin{cases}Ad/T^{BUR}\ if\ Ad>0,\\ 0\ if\ Ad\le 0,\end{cases} \qquad (11)$$

$$ER=\begin{cases}\left|Ad/T^{RL}\right| if\ Ad<0,\\ 0\ if\ Ad\geq 0,\end{cases}\quad Ad=IR-Rep,$$

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

$$DFP=(RMR*Rep)+BFP,\ \frac{\mathrm{d}(DAP)}{\mathrm{d}t}=IFP,$$

where R_i is the increase in the number of successful corrupt deals of one particular corruption type during the time necessary for a counteraction party to report the accomplished corrupt deals; D_i is the number of reported prevented corrupt deals divided by the time necessary to prevent these deals; A_i^{RS} is the successful corrupt deals, which became known; A_i^{S} is the successful corrupt deals; T^{RA} is the time required to report corrupt deals; N^{DA} is the number of prevented corrupt deals; T^{D} is the tile of corruption prevention; FI_i is the part of funds directed to counteract corruption of the i-th type; *Rep* is the reputation; T^{BUR} is the time to enhance reputation; T^{RL} is the time of reputation loss; R^{B} is the basic (initial) reputation; V_i is the cost of corrupt deal of type i; Vul_i is the probability of success of corrupt deals of type i; *DFP* is the financial performance of the anti-corruption party; *RMRC* is the ratio of reputation to monetary rate; *BFP* is the basic financial performance; *DAP* is the accumulated profit of the anti-corruption party; *IFP* is the increase in financial performance, Δt is the time interval between consecutive corrupt deals.

– sub-model of interaction environment:

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

$$SA_i=\begin{cases}\left(C^{A}*AF_i\right)-\left(\left(C^{D}*AF_i\right)/C^{UA}\right)\text{ if } Vul_i>0,\\ 0\text{ if } Vul_i\leq 0.\end{cases}\qquad(12)$$

where C^{A} is the capabilities of corrupt officials; AF_i is the part of corrupt deals of type i; C^{UA} is the cost of one corrupt deal; C^{D} is the capabilities of a counteraction party.

– *sub-model of a corrupt official:*

$$A_i^{AS}(t)-A_i^{AS}(t+1)=B_i\cdot\Delta t,\ \ B_i=A_i^{S}/T^{RA},$$

$$V_i^{P}(t)=A_i^{AS}(t-1),\ \ S_i=\begin{cases}0\ if\ A_i^{AS}-V_i^{P}<1,\\ 1\ if\ A_i^{AS}-V_i^{P}\geq 1,\end{cases}\qquad(13)$$

$$A_i^{F}=$$

$$=S_i\times A_i^{AS}/\sum_{i=1}^{3}S_i\times A_i^{AS},$$

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

$$\frac{\mathrm{d}(AAW)}{\mathrm{d}t}=IAW,$$

where: A_i^{AS} are the accumulated successful corrupt deals of type i; A_i^{S} is the successful corrupt deals of type i; V_i^{P} is the previous value of corruption of type i; S_i is the switch between the kinds of corruption i; P^{A} is the performance of corrupt officials; B_i is the corruption of type i; W^{AA} is the accumulation of well-being of corrupt officials; W^{IA} is the increase in well-being of corrupt officials.

The resulting system of equations describes the behavior of a corrupt official and anti-corruption party, the interaction of which determines the direction of investment of funds in the anti-corruption system, as well as the moments of a change in the direction of funding.

The following data were selected as source data to carry out the simulation experiments: preliminary data on the distribution of different types of corruption, the ratio of funds of corrupt officials and those who oppose corruption, zero initial level of the income from corruption, the probability of successful counteraction to the corruption of the considered types. In particular, it was assumed that the ratio between corrupt deals of the first, second and third types is 1:0.75:0.5. The proposed simulation model is based on the ratios of the number of cases of recorded corruption. The boundary-value of this ratio was 1:1:1. A similar observation can be made regarding the ratio of funds for the implementation of corruption deals and corruption counteraction, while the average value of the income of a corrupt official from a single corruption deal was estimated at 1,000 cond. units. The model is scalable by cost indicators, which under conditions of possible inflation is a reasonable assumption.

Fig. 11, 12 show the results of simulation of the behavior of participants in the corruption process. Fig. 11 shows an increase in the cumulative result of the welfare of corrupt officials.

Fig. 12 shows the results of simulations of successful corruption deals for all three types of corruption.

This graph has an interesting feature. The number of successful corruption deals of corruption type 2 (current educational process) increases sharply in January and June, that is, during the sessions of exams. However, corruption deals of type 1 (corruption related to the work of the admission committee) fall sharply after the completion of the work of admissions committees. A similar dynamic is observed for corruption type 3 – administrative corruption.

This can be explained in part by the fact that the main part of violations may be related to the accommodation of students in dormitories, and the lists for accommodation in dormitories are formed during the work of the admission committee.

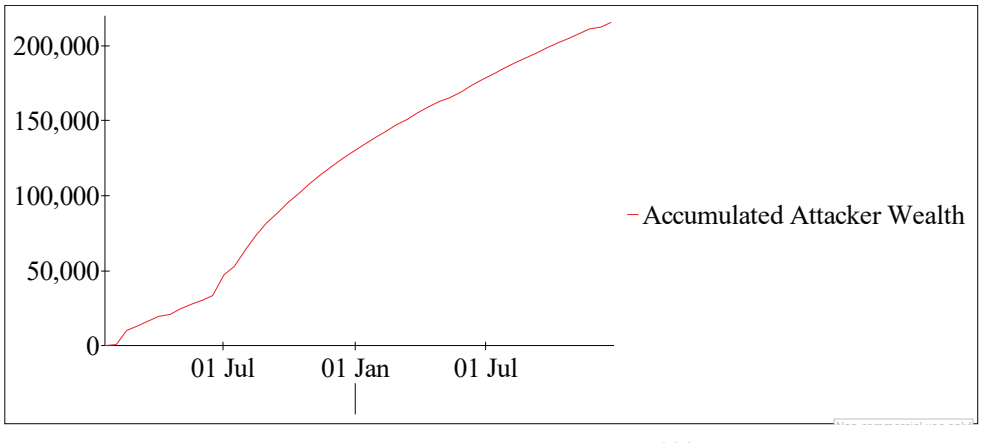

Fig. 11. An increase in the wealth of attackers (1,000 cond. units)

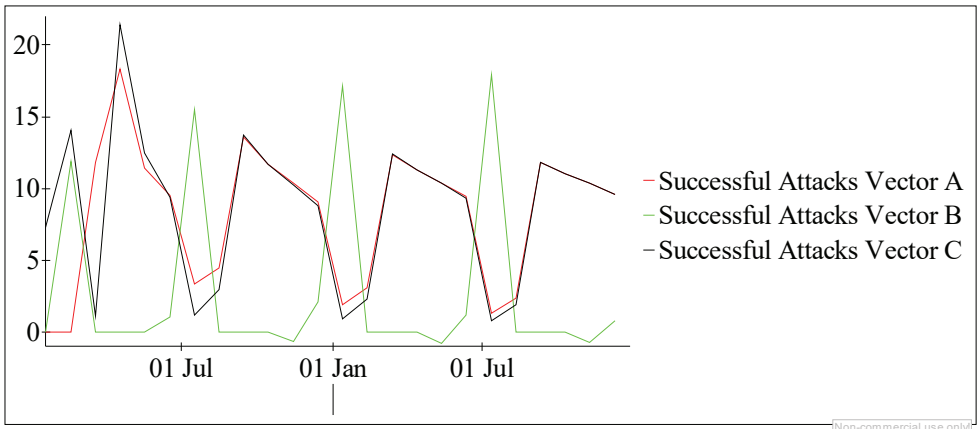

Fig. 12. Distribution of successful corrupt attacks of different types: corruption of type 1 — Vector A; corruption of type 2 — Vector B; corruption of type 3 — Vector C

7. Discussion of the methodological principles of construction and management of CIES in an anti-corruption environment

The operative interaction of a decision-maker (DM) with the corporate information and education system constitutes one of the main operations of the entire technological cycle of management of an innovative and active university, which is considered as a business system. At the same time, the characteristics of a person as an element of the contour are increasingly often becoming a bottleneck in operational management under the existing structure of means and methods of human-machine interaction [64–67].

The way out of this situation is to create a semiotic structure of a corporate information system that allows:

– collecting and complexing information on potential opportunities and threats to normal functioning and their implementation sources;

– processing and storing this information with acceptable degrees of aggregation;

– automatic and/or human-machine assessment of the states of security level and business process environment with the prediction of new opportunities and types of threats;

– automatic and/or human-machine search for solutions on management tools selection initiated by estimates of the states of a control object and its operation environments, as well as unfavorable tendencies of development;

– automatic and/or human-machine optimization from the position of the money spent and the time of found and recommended solutions;

– human-machine decision-making with the possibilities of calling for analysis of both the data that are the basis for the search for proposed managerial solutions, counteraction to corruption, and the used logic and the mathematical methods, on which the search for proposed solutions was based.

The semiotic approach explores the scheme, in which the management body knows:

– not always a determinable set of parameters $\{x\}$, characterizing the current state of a control object and its operating environment;

– a set of the ways of splitting $\{x\}$ into classes of states $K=\{k_1, k_2, ..., k_z\}$, requiring decision making;

– a set of models of solution search $\{M\}$;

– a set of mechanisms of solution search on models – $\{\varphi\}$.

In the implementation of such a scheme, sets $\{k\}$ and $\{M\}$ are dynamically formed from the possibility to get the necessary solutions within acceptable terms, however, the nature of the obtained solutions is qualitative.

The system of counteraction to the corruption of the business process circuit should be based on the concept of human-machine management. This statement follows from an analysis of a set of functions assigned to the system, existing approaches to automation of decision-making processes, as well as the existence of decision-makers united in teams.

Analysis of the problems that must be solved in decision-making systems with intelligent mechanisms for the automatic search for anti-corruption tools shows that:

– the formal apparatus that describes the processes of situation recognition, generation and making decisions in a rapidly changing environment with the elements of uncertainty must be extremely flexible;

– decision-making and generation processes are based not only on quantitative characteristics, but also on the factors that do not always have quantitative measures (psychological, moral, etc.).

Therefore, the preparation of information for anti-corruption decision-making should be seen as a creative act of choice from a combination of possible solutions. At the same time, quantitative factors are combined with the heuristic abilities embedded in the computer that forms the solution. Solutions are based on two components of formal and creative decision-making;

– particular attention should be paid to the decision-making process itself, that is, it is important to know, which components of the management process should be controlled by a DM and which can be implemented by computers;

– the problem of communication between a man and a computer has an important place. The problem has two sides – to meet the information needs of the information available in the system and to participate in the decision-making process. A natural requirement for the means of information presentation is their informativeness and convenience of using the language of communication – proximity to the language of professional vocabulary and its slangs. The form of communication should be a dialogue;

– the problem of education or adaptation of the developed system to the manifestation of new corrupt actions requires the development of a special procedure allowing giving the information presented formally (algorithmically) and informally (expertly). Such a procedure should be human-machine in nature and be applicable to a large class of situations;

– the challenge of designing and generating different versions of software of decision systems requires the development of a special human-machine design technology within this class of systems.

Taking into consideration the nature of the systems of the type in question, based on the ability to adapt and build targeted behavior, we will distinguish between two types of information in the corporate system [3]:

– information that monitors the targeted behavior of a system by organizing processes to recognize corruption, search for and making decisions on counteraction;

– information that is the elements of processing from the side of the above process.

The first type of information will be called *knowledge of the system about the management domain* – models, tasks, algorithms.

The second type of information will be called *data on the state of the system, object, and threat formation environment* – parameters of the system, object, environment, and area of determining these parameters.

Analysis of decision-making processes has made it possible to state the following concepts as a basis [23, 24]:

– *the global logic model of knowledge* as a set of problems, models, and ways of their use to organize processes of targeted recognition of situations of corruption, generation, and decision-making on counteraction;

– *the area of interpretation of the global logical knowledge model* as a structured and orderly dynamic set of attributes that characterizes the parameters of a business process system, object, and operating environment;

– *a team of system analysts, experts* who, using recognition and communication tools, can determine and describe the elements of the global logical knowledge model and the scope of its interpretation to the extent sufficient to solve the problems that can be posed in any problematic situation.

The following characteristics of the model should be taken into consideration when developing the concept:

Expert character as the basis for shaping the goals of the business process system, the models that are the region of solution search, rules of searching for and making decisions to protect the contour of business processes.

Associative character is the basis for automatic accumulation, the generalization of information, and adaptation of a university as a business system to the changing operating environment.

Multi-alternativeness as a basis for displaying all possible ways to find solutions.

Semiotics as a basis for the development of mechanisms for integrating heterogeneous information about an object of protection from corruption and the environment of its formation.

Communication capability as the basis for the implementation of the dialogue means of the system's communication with the DM.

Virtuality as the basis for reflecting the globality of information, which is characterized by territorial disunity and multi-layered sources of information obtaining, storing, and using.

Performance as the basis for the implementation of the model of providing a necessary security level in software and hardware environments.

The resulting model has a range of new properties, for example, it is both a means of solving problems facing the system of problems and the methodology for designing and implementing such systems. The team of experts has both formal and informal knowledge of the management domain. At the same time, each expert performs a certain educating function in the team. This makes it easy for it to design and fill a knowledge model, to separate a specific local logical knowledge model, and have an access to global models of knowledge and data. The existence of experts allows constructing, in addition to procedures for recognition, development, and decision-making:

– procedures for identifying consistent knowledge, using dynamically changing expert groups; create expert models for developing solutions to different classes of corruption situations;

– to simulate any combination of centralized and decentralized decision-making; to achieve greater commonality, which makes it possible to implement different methods of problem-solving. In addition, such a team has the capability of formalizing communication between experts and build standard means of communication on this basis. With these tools, different modes of interaction are organized, from the explicit application of one expert to another to implicit application, when the recipient is determined by the function he performs.

The existence of a set of tasks, models, and knowing how to use them in specific situations of generating and making decisions makes it possible to develop unified tools to describe such information and organization of their use by a system. Such tools include the means of linguistic and software maintenance: the languages of determining a logical knowledge model (LKM) and the manipulation of the elements of a logical knowledge model (LKM). The definition of knowledge involves the introduction of new types of information, such as a model, a task. The manipulation of knowledge is based on planning the processes of searching solutions in the global knowledge model through the use of, first and foremost, a goal-setting mechanism.

The considered concept is well consistent with the nature of complex human-machine decision-making systems and makes it possible, using the knowledge of experts and programmers:

– to develop knowledge about possible types of corruption for the appropriate contour of business processes;

– to construct the models of recognition, classification of state, goal setting, generation and making managerial decisions to combat corruption;

– to construct a functionally complete set of computational algorithms that characterize a specific area of anti-corruption;

– to "fill" the anti-corruption software system with specific content;

– to design and generate the system's software and organize its problematic orientation.

Summing up the above, we can conclude that the considered concept fully meets the problems of managing complex social objects, methods, and theories of construction of large management software complexes, security systems of business processes functioning.

Ensuring the required level of combating corruption of the contour of business processes will be considered as a human-machine activity to determine the states of the protected object. This requires decision-making related to the search and choice by purposefully coordinating *models of behavior of all participants in the business process* included in a computer – M_1 and the one a DM has – M_2.

Model representation is determined by knowledge about anti-corruption methods and mechanisms, objectives and limitations of the parties, objective and subjective preferences for choosing the ways of achieving goals, and assessing the degree of their applicability.

The interactivity of human interaction with the system is organized by introducing the concept of a human-machine situation that requires decision-making S_y and determining this concept of a set of attributes. The nature of this activity,

on the one hand, is set by a person by managing the processes of setting the task of tracking the progress of its solution. On the other hand, the system clarifies the correctness of the set tasks, offers alternative ways to solve them, using "the expertise" of finding solutions, reflected in its model. Thus, a human and a system interact as partners, aligning their methods for solving the problems of ensuring counteraction corruption of the required level.

Symbiosis will be optimal only when the system operation is organized in the mode of "intellectual" adviser of a person. At the same time, the system performs routine functions of automatic situation recognition, as well as the search for countermeasures based on information both received from experts and using system knowledge.

This knowledge exists in the system in the form of two kinds of structured sets {computational and theoretic multiple}, {dialogue and *expert*} (*logical-algebraic and logical-linguistic*) models of recognition of the situation of possible manifestation of corrupt actions and search for the tools of counteracting it. The first kind of models is determined on the situations, for which it is possible to find the algorithm relating the unknown parameters with the assigned ones, and the range of variants is not large. The second kind of models serves to look for the decisions, dependent on situations and the range of decisions is extremely large. It can be said that computing and theoretic-multiple models are analogs of calculation operations when searching for solutions, and dialogue and expert are the analogs of the methods of searching for solutions.

The capabilities of each of the interacting parties of the business process are determined by the completeness of behavior, decision-making procedures, and the model basis for decision-making procedures. At the same time, decision-making and behavior processes are considered as semiotic (sign). The sequence of steps (related by cause-and-effect connections, temporal, spatial, and other relationships) of finding management solutions for each problem situation, used in this case, is considered as the solution search logic.

At every step of the interaction between a DM and a decision support system of one of the parties, a request is formed in the form of a problem situation and/or a subset of algebraic operations of the model in accordance with the decision search logic. The purpose of a decision-making system is to find the interpretation of these operations in terms of its model, their execution, and the generation of response request.

Formal representation of the model of DM's behavior in operative decision-making is assigned by the following expression

$$M_1=<BT, DM, ИТ>, \quad (14)$$

where

$$BT=<L_{BT}, ACS, \Theta>$$

– behavior theory (knowledge model of a system);

$$DM=<x^z, b^z, f^z, p^z>$$

– information data model, describing a system;

$$I=<UI_1, CI_2>$$

– interpretation of *BT* in *DM*.

Here $L_{BT}=L_{KDL}\cup L_{DDL}$ is the language of description of the behavior model, that is the combination of knowledge and data determining languages; *ACS* is the axioms of the theory; Θ is the rules of statement inference in theory; x^z, b^z are the set of variables and constants of state; f^z, p^z are the set of functional and predicate variables of state; UI_1 is the user's interpretation of the elements of the system knowledge model, assigning expertly the corresponding rules for setting the match between the syntactic structure of the language elements L_{BT} and their sense in the considered domain (semantic of DM); CI_2 is the machine interpretation of the elements, assigning expertly the match between the semantic structure of the language elements L_{BT} and their truth at each current moment of the search for decisions (pragmatics).

The formal model of the behavior of a business process participant, depending on the limitations imposed on the rules of inference making, can be described by means of the logic of first-order predicates, production, and algorithmic systems. Indeed, there are no restrictions on the application of inference rules in the logic of predicates. Any inference rule is appropriate for any derived statement if this statement allows using it. Production systems, also based on the logic of predicates, have additional conditions on the applicability of an inference rule. These conditions may change in the course of operation of a production system, depending on the receipt of some information during the inference process. In algorithmic systems, the sequence of rules is determined unequivocally. The language of first-order predicate logic and the language of information processing algorithms were selected as the rules of statement inference in theory. The inference rules in the logic of predicates, their modifications in the system of products and algorithmic rules were chosen as the rules of statement inference in theory.

The relationship of the behavior model with challenging situations and the tasks of finding solutions is achieved by taking into consideration the logical sequence of the stages of the DM's work and separation of a set of decision-making procedures typical of a DM.

This set of procedures can be presented as the following sequence (Fig. 13).

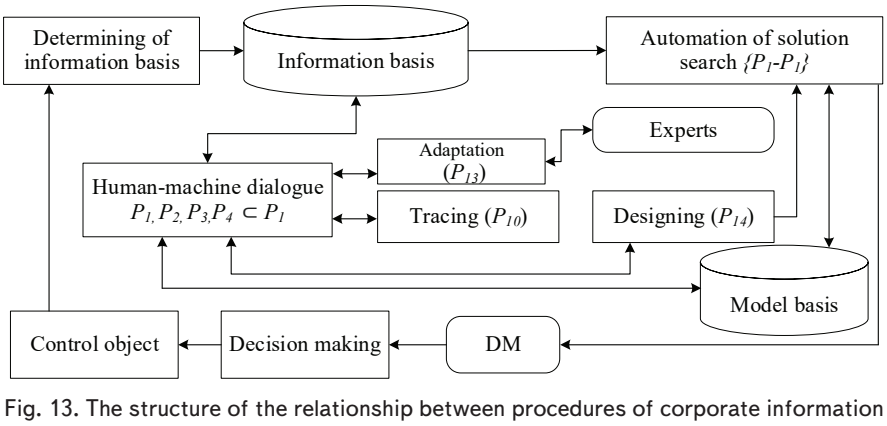

Fig. 13. The structure of the relationship between procedures of corporate information and educational procedures under conditions of anti-corruption environment

Procedure of situation classification:

P_1=<S, J, K_p, K_s>,

where S is the situation assigned by some ratio on a set of elements I; J is the set of expert preferences on choosing the classification rules, assigned on set $\{S \times K_s\}$; K_p is the set of classification rules – deciding procedures; K_s, is the set of classes of situations, for which there are decision search models;

– *model classification procedure* makes it possible to determine the set of decision-making models, using the computing on which, it is possible to find the required solutions to ensure the required level of anti-corruption:

P_2=<S, K_s, A_l, M_1>,

where A_l is the set of alternatives of choosing solution search models, weight coefficients of which depend on S and K_s, can be assigned by a person in the interactive mode of working with a system; M_1 is the set of decision search model;

– *procedure of generating the strategies of solution search goal* makes it possible to determine a set of local and (or) global aims of the system of business processes that are necessary to achieve with the help of decisions found in this class of situations:

P_3=<S, K_s, G, Cr, Str>,

where G is the set of current goals facing a managing system; Cr is the set of goal achievement criteria (both goals and criteria can vary and change over time); Str – is the set of strategies of decision search goal;

– *procedure of the search for target managing decisions* makes it possible to organize the search for decisions for each problem situation according to the goals and criteria of ensuring the contour of business processes safety:

P_4=<S, Str, M_1, R_G>,

where R_G is the set of target management solutions that can be found in the solution search model (database) M_1, adjusted to current situation $s_i \in S$ when using strategy $str_i \in Str$. This procedure performs two functions – a planner of a computing sequence of solution search and a decision-maker. The former function implies the formation of a decisive sequence of programs, the latter – organization of fulfillment of these programs and getting managerial recommendations in a specific computing environment;

– *procedure of determining the possible decision implementation outcomes* makes it possible to assign attainability of local and (or) global management goals during the realization of certain decisions on corruption counteraction. This is achieved by means of the organization of computing on the model of admissible decision-making region – M_{ADA}, determining this region – O_{ACA}, in accordance with goals G and criteria Cr, characteristic for the given decision-making level. This procedure is set as:

P_5=<S, R_G, G, Cr, M_{ADA}, O_{ACA}, R_{G1}>,

where R_{G1} is the set of those managing decision, which are satisfactory outcomes, that is, the outcomes, during the implementation of which it is possible to achieve local and (or) global management goals;

– *procedure of decisions substantiation* enables assessment of decision quality (their optimality) by organizing computing on the model for determining the optimal decision-making region (M_{ODA}) to choose the region of choosing the optimal management decisions (O_{OD}) in accordance with goals and criteria. The element of tuple R_{G1} is the set of those management decisions, which satisfy O_{OD} and can be, first of all, recommended to be implemented. This procedure

P_6=<S, R_{G1}, G, Cr, M_{ODA}, O_{OD}, R_{G2}>;

– *procedure of decision synthesis* allows the reduction of the number of simultaneously recommended countermeasures, no matter how many situations are analyzed by the system at a time. In addition, the procedure ranks the decisions made by a DM, both on the information received from procedures P_5, P_6, and using a set of preferences on "narrowing" set R_G. These preferences can be assigned expertly. The procedure is set in the form of

P_7=<S, R_{G2}, O_{ACD}, O_{ODR}, R>;

Information for a DM after operation of this procedure is given in the form of <$\{S\}$=>$\{R, O_{ACD}, O_{ODR}\}$. A DM may connect the current situation with the necessary decisions taking into account their belonging to O_{ACD} and O_{ODR}, assigning R_{G2};

– *decision-making procedure* makes it possible to organize the process of human-machine interaction in order to make one decision that has to be implemented. At the same time, a DM can choose one of the system's recommended countermeasures or make his own, different from the recommended, R_G, which should be reported to a system. If $R_G \cap \bar{R} = 0$, this solution can be implemented. Here, $\bar{R} = R_G \cap R_{G1} \cap R_{G2}$ is the forbidden set of decisions. Formally, this procedure is

P_8=<S, R, $\bar{R}$, R_G>;

– *the procedure of decision implementation assessment* makes it possible to assess the effectiveness of made and implemented decisions in order to correct (in training or self-learning mode) of the system knowledge model and transferring a part of information of the kind {<situation>–<decision>} from the sphere of a decision-making system to the sphere of automatic decision implementation. This procedure

P_9=<S, $R \cup R_G$, M_1, P_{13}>,

where P_{13} is the procedure of learning (self-learning) of a system and correction of its knowledge model M_1;

– *the decision-tracing procedure* makes it possible to monitor the *logic of machine reasoning* when searching for solutions and the used information basis. This procedure gives back to a DM the observability property, that is, the possibility of establishing any relationship on the elements of decision-making procedures. The tracing procedure is based on a modification of the orderly procedure sequence of P_1–P_9. The modification is to introduce in each procedure P_i of the statement that the results obtained with its help are correct. Formally, this procedure is

P_{10}=<μ_1:P_1, μ_2:P_2, …, μ_9:P_9, Cor>,

where μ_1, μ_2, ..., μ_9 are the conditions of implementation (statement on correctness) of procedures P_1, P_2, ..., P_9 respectively, written down in the form of μ_i:P_i. Using the elements of this tuple, a human has an opportunity to verify the psychological correctness of found solutions by means of interaction with the system. The statements, belonging to *Cor,* determine the consistency of logic, included in the base of models and procedures of a computer and a DM, that is, they enable a system to report to a DM that the next cycle of the search for and making decisions is completed;

– *procedure of the information dialogue* enables organizing the human-machine interaction of a DM with the system with a view to obtaining the information necessary to him. This procedure

$$P_{11}=<P_1, P_2, P_3, P_4>,$$

where P_1–P_4 are the considered procedures, in which the following substitutions were performed: S/R_A, M_1/M_A, C/C_D, G/G_D; R/R_0; R_D are the set of requests from a DM; $M_A \in M_1$ is the set of models of response search by the requests determining regions; Str_D is the set of strategies of the decision search, ranked by set M_A; G_D is the set of current goals; R_O is the set of responses given by a DM during the reaction of a system to a request;

– *the procedure of determining the information basis for decision making* is linked to the information collecting system in order to organize information processing and recording it into the information model (database) of the systems. Formally, this procedure:

$$P_{12}=<S, P_1, P_2, P_3, P_4, M_1, M_D>,$$

where M_D is the information model, storing the current state of an object;

– *the procedure of adaptation/ learning* enables the organization of the automated adjustment of a system to the region of ensuring counteraction.

$$P_{13}=<L_L, E_K, E_D>,$$

where L_L is the mechanism of correction of models of knowledge and databases (means of knowledge and data description), allowing linking information in its machine representation; E_K, E_D are the set of elements of the level of a knowledge and data model;

procedure of automated design, or a dialogue system of the automated designing a system of ensuring corruption counteraction. For a DM and systemic analysts-designers, this procedure

$$P_{14}=<S, L_{DKL}, L_{DML}, L_{LDL}, M^{Comp}>,$$

where S is the design situation from the class of situations of human-machine designing, reflecting the object-oriented statement of a problem of construction of the information and model basis; L_{DKL}, L_{DML}, L_{DDL} are the language means for describing the elements of the model knowledge and data basis; M^{Comp} is the machine representation of the information and model basis.

Fig. 14 shows the structural and logical block diagram of the methodological basis of the construction of the CIES of the IAU under conditions of corruption counteraction. To construct a conceptual synergistic model of security of the CIES of the IAU, we will use the updated classifiers of threats to cyber-physical (CFS) and information and communication (ICS) systems, proposed in paper [64].

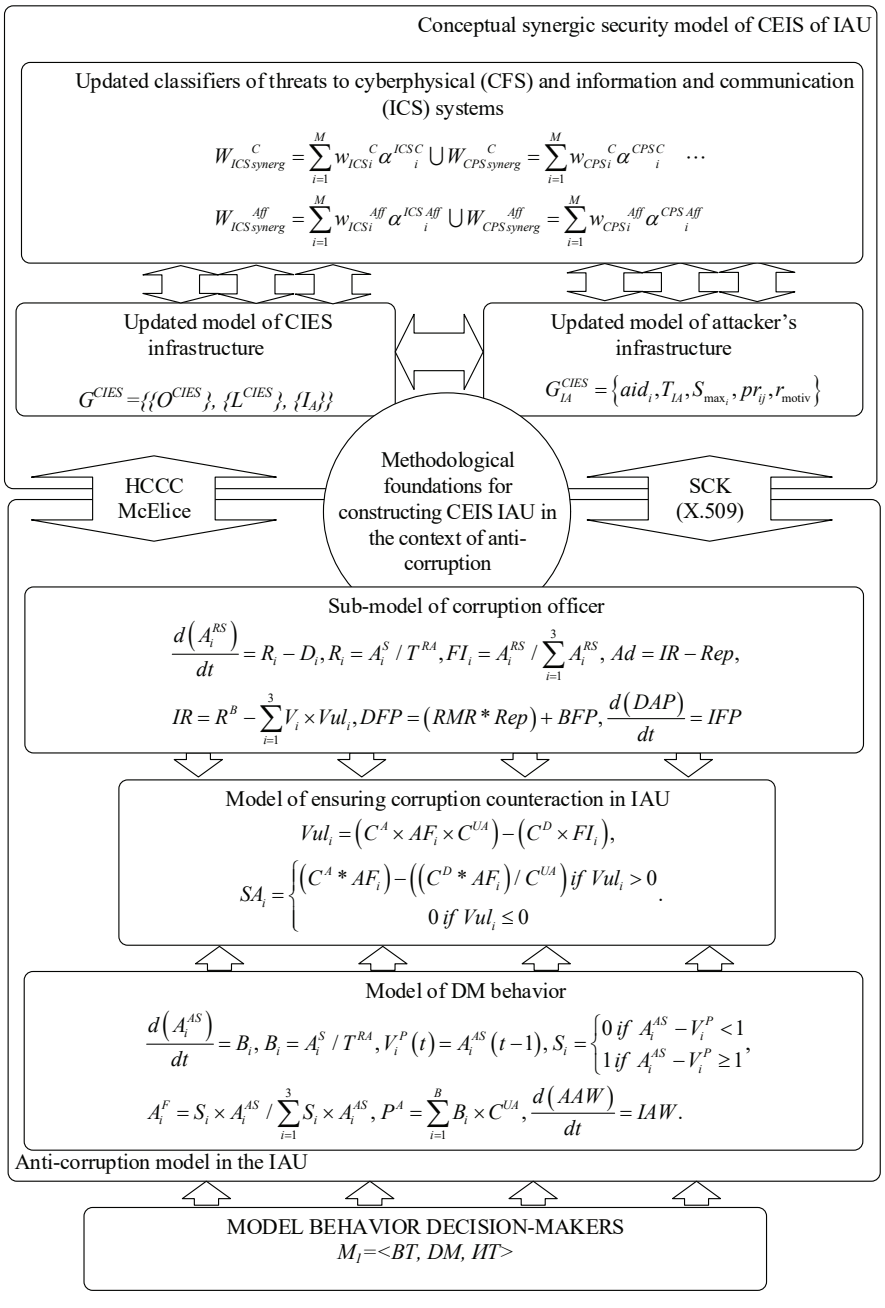

Fig. 14. Structural and logical scheme of methodological foundations for the construction of CIES of IAU in the face of corruption counteraction

Thus, by proposing a structural and logical scheme of methodological principles for constructing the CIES of IAU in an anti-corruption environment, it is possible to automate the control of an electronic document and e-education services at all levels of the university's hierarchical management structure. The main automation mechanisms are the services based on the use of KCC and commercial implementation of crypto-algorithms. This approach provides the required level of security services, effective control of corruption counteraction in the face of modern cyber threats (both internal and external).

The main limitations of the conducted simulation are the subjectivity of the choice of corruption types and the assessment of modern threats to corporate university universities.

Subsequent development is seen in carrying out the studies to increase the level of corruption counteraction in the IAU based on a pilot project of implementation of the principles of constructing and managing the corporate information and educational system of an innovative and active university.

8. Conclusions

1. A distinctive feature of the modern stage of modernization of the higher education system in the world is the change of the paradigm of the functioning of universities and the emergence of the phenomenon of "a university of entrepreneurial, innovative and active type". This paradigm is based on the emergence of a distributed system of production and dissemination of knowledge. This, in turn, predetermines the need for broad interaction of universities with various external stakeholders based on the use of modern information and communication technologies. Under these circumstances, the activities of universities, their culture of responsibility, and the system of values are changing significantly. The competitiveness and relevance of a university are assessed mainly in accordance with its contribution to the economic development of a country and humanity in general. The result of studying the connection between the change of the university mission and industrial revolutions, the generalization of the specific features of the spirals of interaction between a university and society was the development of an operating model of interaction of a university with the main stakeholders. A distinctive feature of the presented model is a new understanding of the mission of a university, namely, universities are called to serve society by supporting the economy and improving the quality of life of its citizens. Based on this, the authors' interpretation of the innovative and active university (IAU) was presented. The IAU implies an entrepreneurial structure that has resource readiness to contribute to the accelerated development of the economy and society through the transfer of knowledge and technologies generated at the university based on partnership interaction with major stakeholders. The set of the latter is formed by labor market actors, governmental and public organizations. The following was separated as the dominants of the IAU activity: science as a tool for generating new knowledge; education as a way of construction of the intellectual potential of society; interaction with industry, government, society as a means of ensuring the sustainable development of the nation.

2. The proposed Concept of corruption counteraction not only takes into consideration current tendencies in e-education, goals and objectives, but also provides counteraction to the elements of corruption and integrated hybrid threats.

The basis of corruption counteraction is a digital signature of KCC based on the X-509 standard, which provides the security service – authentication. To ensure security services, privacy, and integrity, it is proposed to use the commercial implementation of McEliece and Niederreiter crypto-code designs on the MES and defected codes. This approach ensures the required levels of confidence, efficiency and crypto resistance, as well as counteracting to crypto book-marks.

The proposed synergistic model of CIES security makes it possible not only to take into consideration synergies and hybridity of modern threats but also to form preventive counteraction measures based on the timely identification of critical points in the infrastructure of CIES and the formation of AIPS.

3. The model for ensuring corruption counteraction that reflects the scenarios of the behavior of corruption process participants and anti-corruption bodies was developed.

The purpose of developing a model of the behavior of various participants in corrupt actions was defined as ensuring the possibility of scenario simulation of the behavior of the parties. This goal statement ultimately influences the choice of the direction of anti-corruption actions implementation and investment of limited funds in anti-corruption programs.

The main result of the conducted simulation of scenarios of the behavior of the corruption process parties is the dynamics of the distribution of corrupt deals over time and by the corruption types. This makes it possible to effectively redirect the university's limited resources to anti-corruption activities.

Acknowledgements

The article was prepared using the results of studies within the applied scientific research work No. 46/2020-2021 "Development of the methodical and model-information support to the construction of a university of innovative type based on the quality of education and corruption counteraction" funded from Ukraine's State budget.

References

1. Zakon Ukrainy vid 1 lypnia 2014r. # 1556-VII «Pro vyshchu osvitu». Available at: https://zakon.rada.gov.ua/laws/show/1556-18#Text
2. Ukaz Prezydenta Ukrainy «Pro Natsionalnu doktrynu rozvytku osvity» vid 17 kvitnia 2002 r. Available at: https://zakon.rada.gov.ua/laws/show/347/2002#Text
3. Ukaz Prezydenta Ukrainy «Pro Natsionalnu stratehiyu rozvytku osvity v Ukraini na period do 2021 roku», vid 25 chervnia 2013 r. Available at: https://zakon.rada.gov.ua/laws/show/344/2013#Text
4. Kontseptsiya rozvytku osvity Ukrainy na period 2015–2025 rr. Proekt. Available at: http://tnpu.edu.ua/EKTS/proekt_koncepc.pdf

5. Kontseptualni zasady reformuvannia publichnoho finansuvannia ta upravlinnia zakladamy vyshchoi osvity. Available at: https://drive.google.com/file/d/1obC0K1NMhh9soat7LK9y-ughV4n070-h/view
6. Engaging for Excellence: Generating alumni support for higher education. Advancement Metrics and research for education (2018). Washington: Case AM Atlas, 58. Available at: https://www.case.org/system/files/media/file/Engaging_for_excellence_2018_final.pdf
7. Gaebel, M., Zhang, T., Bunescu, L., Stoeber, H. (2018). Trends 2018: Learning and teaching in the European Higher Education Area. Geneva: European University Association, 109. Available at: https://eua.eu/downloads/publications/trends-2018-learning-and-teaching-in-the-european-higher-education-area.pdf
8. Taneja, P., Safapour, E., Kermanshachi, S. (2018). Innovative Higher Education Teaching and Learning Techniques: Implementation Trends and Assessment Approaches. 2018 ASEE Annual Conference & Exposition Proceedings. doi: https://doi.org/10.18260/1-2--30669
9. Becker, B. A., Eube, C. (2018). Open innovation concept: integrating universities and business in digital age. Journal of Open Innovation: Technology, Market, and Complexity, 4 (1). doi: https://doi.org/10.1186/s40852-018-0091-6
10. Kumar, S., Gokhale, A., Bhattacharya, S., Mathai, V. (2018). University of the Future: Bringing Education 4.0 to life. New Delhi: FICCI, Ernst & Young LLP, 60.
11. Grenčíková, A., Španková, J., Petrušová, D. (2017). THE CHALLENGES AND TRENDS IN HIGHER EDUCATION. CBU International Conference Proceedings, 5, 616–621. doi: https://doi.org/10.12955/cbup.v5.995
12. Estermann, T. (2013). Setting the context: University Autonomy & Funding in Europe: ATHENA Workshop Ukraine – Fostering Sustainable and Autonomous Higher Education Institutions.
13. Seyfried, M., Pohlenz, P. (2018). Assessing quality assurance in higher education: quality managers' perceptions of effectiveness. European Journal of Higher Education, 8 (3), 258–271. doi: https://doi.org/10.1080/21568235.2018.1474777
14. Elken, M., Stensaker, B. (2018). Conceptualising "quality work" in higher education. Quality in Higher Education, 24 (3), 189–202. doi: https://doi.org/10.1080/13538322.2018.1554782
15. Oppliger, R. (2005). Contemporary Cryptography. Artech House computer security series, 530.
16. Clark, B. (1998). Creating Entrepreneurial Universities: Organizational Pathways of Transformation. Oxford/New York: Pergamon Elsevier.
17. Gibbons, M. (1998). Higher Education Relevance in the 21st Century. The World Bank, 73. Available at: https://eric.ed.gov/?id=ED453721
18. Huisman, J., Smolentseva, A., Froumin, I. (Eds.) (2018). 25 Years of Transformations of Higher Education Systems in Post-Soviet Countries. Palgrave Studies in Global Higher Education. doi: https://doi.org/10.1007/978-3-319-52980-6
19. Seniwoliba, J. A., Boahene, B. E. (2015). Manifestation of corruption in higher education: the role of the University administrator. Research Journal of Educational Studies and Review, 1 (3), 78–88.
20. Muzalevskaya, E. A. Proyavleniya korrupcii v sisteme obrazovaniya. Available at: http://www.mosgu.ru/nauchnaya/publications/SCIENTIFICARTICLES/2006/Mazulevskaja/
21. Korrupciya radi vyzhivaniya. Available at: https://rian.com.ua/view/20151229/1002827333.html
22. Kak ochistit' sistemu upravleniya obrazovaniem. Available at: http://ru.osvita.ua/vnz/high_school/46714/
23. Zahorskyi, V. S. (Ed.) (2011). Upravlinnia yakistiu osvity u vyshchykh navchalnykh zakladakh. Ch. 1: Teoretychni zasady formuvannia system upravlinnia yakistiu nadannia osvitnikh posluh. Lviv: LRIDU NADU, 136.
24. Revak, I. O. (2011). Koruptsiya: teoretyko-metodolohichni zasady doslidzhennia. Lviv: LvDUVS, 220.
25. Rimskiy, V. L. Korrupciya v sisteme obrazovaniya Rossii. Available at: https://imrussia.org/media/pdf/Research/Vladimir_Rimsky__Corruption_of_the_Russian_Education_System.pdf
26. Shevchenko, V. M. Features of education from the mechanisms of state administration, higher educational establishments in the conditions of eurointegration and innovative development of Ukraine. Available at: http://www.kbuapa.kharkov.ua/e-book/db/2010-1/doc/5/07.pdf
27. Klein, E. (2012). Academic Corruption and Reform in Russia and Ukraine. Governance Failure and Reform Attempts after the Global Economic Crisis of 2008/09. Case Studies from Central and Eastern Europe. Stuttgart, 173–190.
28. Rumyantseva, N. L., Logvynenko, O. I. (2018). Ukraine: Higher Education Reforms and Dynamics of the Institutional Landscape. 25 Years of Transformations of Higher Education Systems in Post-Soviet Countries, 407–433. doi: https://doi.org/10.1007/978-3-319-52980-6_16
29. Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., Zimbelman, M. F. (2011). Fraud examination. Cengage Learning, 696.
30. Christensen, C. M., Eyring, H. (2011). The Innovative University: Changing the DNA of Higher Education from the Inside Out. Available at: http://forum.mit.edu/wp-content/uploads/2017/05/FF12innovUniv.pdf
31. Mokyr, J., Vickers, C., Ziebarth, N. L. (2015). The History of Technological Anxiety and the Future of Economic Growth: Is This Time Different? Journal of Economic Perspectives, 29 (3), 31–50. doi: https://doi.org/10.1257/jep.29.3.31
32. Cai, Y., Etzkowitz, H. (2020). Theorizing the Triple Helix model: Past, present, and future. Triple Helix Journal, 1–38. doi: https://doi.org/10.1163/21971927-bja10003

33. Etzkowitz, H., Viale, R. (2010). Polyvalent Knowledge and the Entrepreneurial University: A Third Academic Revolution? Critical Sociology, 36 (4), 595–609. doi: https://doi.org/10.1177/0896920510365921
34. Wang, Y., Tang, B. (2020). Research and Practice on the Collaborative Education System for the Innovation and Entrepreneurship of E-commerce Major. 2020 International Conference on Big Data and Informatization Education (ICBDIE). doi: https://doi.org/10.1109/icbdie50010.2020.00053
35. Valencia, A. V., Cázares, M. del C. T. (2016). Academic and research networks management: challenges for higher education institutions in Mexico. International Journal of Educational Technology in Higher Education, 13 (1). doi: https://doi.org/10.1186/s41239-016-0013-2
36. Cappiello, G., Pedrini, G. (2017). The performance evaluation of corporate universities. Tertiary Education and Management, 23 (3), 304–317. doi: https://doi.org/10.1080/13583883.2017.1329452
37. Margherita, A., Secundo, G. (2011). The stakeholder university as learning model of the extended enterprise. Journal of Management Development, 30 (2), 175–186. doi: https://doi.org/10.1108/02621711111105768
38. Meissner, D., Erdil, E., Chataway, J. (Eds.) (2018). Innovation and the Entrepreneurial University. Springer. doi: https://doi.org/10.1007/978-3-319-62649-9
39. Carayannis, E. G., Campbell, D. F. (2012). Mode 3 Knowledge Production in Quadruple Helix Innovation Systems. Springer. doi: https://doi.org/10.1007/978-1-4614-2062-0
40. Guerrero, M., Toledano, N., Urbano, D. (2011). Entrepreneurial universities and support mechanisms: a Spanish case study. International Journal of Entrepreneurship and Innovation Management, 13 (2), 144. doi: https://doi.org/10.1504/ijeim.2011.038856
41. Woozley, A. (2020). Theory of Knowledge: An Introduction. Routledge, 194. doi: https://doi.org/10.4324/9781003074663
42. Cassiman, B., Valentini, G. (2015). Open innovation: Are inbound and outbound knowledge flows really complementary? Strategic Management Journal, 37 (6), 1034–1046. doi: https://doi.org/10.1002/smj.2375
43. Dodgson, M., Hughes, A., Foster, J., Metcalfe, S. (2011). Systems thinking, market failure, and the development of innovation policy: The case of Australia. Research Policy, 40 (9), 1145–1156. doi: https://doi.org/10.1016/j.respol.2011.05.015
44. Wang, C., Rodan, S., Fruin, M., Xu, X. (2014). Knowledge Networks, Collaboration Networks, and Exploratory Innovation. Academy of Management Journal, 57 (2), 484–514. doi: https://doi.org/10.5465/amj.2011.0917
45. Andreeva, T., Kianto, A. (2012). Does knowledge management really matter? Linking knowledge management practices, competitiveness and economic performance. Journal of Knowledge Management, 16 (4), 617–636. doi: https://doi.org/10.1108/13673271211246185
46. Alfalih, A. A., Ragmoun, W. M. (2020). The role of entrepreneurial orientation in the development of an integrative process towards en-trepreneurship performance in entrepreneurial university: A case study of Qassim university. Management Science Letters, 1857–1872. doi: https://doi.org/10.5267/j.msl.2019.12.033
47. The World's Most Innovative Universities 2019. Available at: https://www.reuters.com/innovative-universities-2019
48. A Guiding Framework for Entrepreneurial Universities. Available at: https://www.oecd.org/site/cfecpr/EC-OECD%20Entrepreneurial%20Universities%20Framework.pdf
49. European Commission (EC) (2013). Entrepreneurship 2020 Action Plan: Reigniting the Entrepreneurial Spirit in Europe, European Commission, DG Enterprise & Industry, COM (2012) 795 final, Brussels, Belgium.
50. The entrepreneurial university: from concept to action (2013). National Centre for Entrepreneurship in Education (NCEE). Available at: https://ncee.org.uk/wp-content/uploads/2018/01/From-Concept-To-Action.pdf
51. The Entrepreneurial University of the Year 2014 (2014). National Centre for Entrepreneurship in Education (NCEE). Available at: http://ncee.org.uk//?s=Entrepreneurial+University+of+the+Year+2014
52. Hryshchuk, R., Yevseiev, S., Shmatko, A. (2018). Construction methodology of information security system of banking information in automated banking systems. Vienna: Premier Publishing s. r. o., 284. doi: https://doi.org/10.29013/r.hryshchuk_s.yevseiev_a.shmatko.cmissbiabs.284.2018
53. X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. Available at: https://www.itu.int/rec/T-REC-X.509/en
54. Dudykevich, V. B., Maksimovich, V. N., Mikitin, G. V. (2016). Strategiya bezopasnosti kiberfizicheskih sistem. Informacionnye tekhnologii v upravlenii, obrazovanii, nauke. Kharkiv: Vid-vo FOP V.V. Petrov, 286–300.
55. Aktual'nye kiberugrozy – 2017: trendy i prognozy (2018). Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2017/
56. Aktual'nye kiberugrozy – 2018. Trendy i prognozy (2019). Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/
57. Aktual'nye kiberugrozy: itogi 2019 goda (2020). Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/
58. Sardak, S. E. (2018). Struktura sredy i urovney upravleniya social'no-ekonomicheskih sistem. Problemy sozdaniya informacionnyh tekhnologiy, 28, 57–64.

59. Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., Scarfone, K. (2016). Guide for cybersecurity event recovery. NIST. doi: https://doi.org/10.6028/nist.sp.800-184
60. Yevseiev, S., Hryhorii, K., Liekariev, Y. (2016). Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system. Eastern-European Journal of Enterprise Technologies, 6 (4 (84)), 11–23. doi: https://doi.org/10.15587/1729-4061.2016.86175
61. Yevseiev, S., Korol, O., Kots, H. (2017). Construction of hybrid security systems based on the crypto-code structures and flawed codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (88)), 4–21. doi: https://doi.org/10.15587/1729-4061.2017.108461
62. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S. et. al. (2018). Practical implementation of the Niederreiter modified cryptocode system on truncated elliptic codes. Eastern-European Journal of Enterprise Technologies, 6 (4 (96)), 24–31. doi: https://doi.org/10.15587/1729-4061.2018.150903
63. Yevseiev, S., Ponomarenko, V., Ponomarenko, V., Rayevnyeva, O., Rayevnyeva, O. (2017). Assessment of functional efficiency of a corporate scientificeducational network based on the comprehensive indicators of quality of service. Eastern-European Journal of Enterprise Technologies, 6 (2 (90)), 4–15. doi: https://doi.org/10.15587/1729-4061.2017.118329
64. Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O. et. al. (2020). Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 3 (9 (105)), 6–19. doi: https://doi.org/10.15587/1729-4061.2020.205702
65. Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? Information Security Technical Report, 14 (4), 186–196. doi: https://doi.org/10.1016/j.istr.2010.04.004
66. Kraemer, S., Carayon, P., Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security, 28 (7), 509–520. doi: https://doi.org/10.1016/j.cose.2009.04.006
67. Bowen, B. M., Devarajan, R., Stolfo, S. (2011). Measuring the human factor of cyber security. 2011 IEEE International Conference on Technologies for Homeland Security (HST). doi: https://doi.org/10.1109/ths.2011.6107876