УДК 378

A. N. Privalov, Dr. Sc. (Tech.), Prof.,
J. I. Bogatyreva, Dr. Sc. (Ed.), Assoc. Prof.,
V. A. Romanov, Dr. Sc. (Ed.), Prof.

Russian State Tula State Pedagogical University, Tula, Russia, e-mail privalov.61@mail.ru

SYSTEMATIC APPROACH TO THE ORGANIZATION OF SAFE INFORMATION AND EDUCATION ENVIRONMENT IN THE HIGHER EDUCATIONAL INSTITUTIONS

О. М. Привалов, д-р техн. наук, проф.,
Ю.І. Богатирьова, д-р пед. наук, доц.,
В. О. Романов, д-р пед. наук, проф.

ФДБОУ ВПО „Тульський державний педагогічний університет ім. Л. М. Толстого", м. Тула, РФ, e-mail privalov.61@mail.ru

СИСТЕМНИЙ ПІДХІД ДО ОРГАНІЗАЦІЇ БЕЗПЕЧНОГО ІНФОРМАЦІЙНО-ОСВІТНЬОГО СЕРЕДОВИЩА У ВНЗ

Purpose. The application of the systematic approach to the organization of safe information and education environment in higher educational institutions.

Methodology. The study and scientific and technical analysis of literature on the problem under study, archival research, modelling, research and generalization of the effective experience of the application of the systematic approach in educational professional institutions.

Findings. The creation of a safe informational environment in the educational professional organization is the necessary condition to provide comfortable professional training of prospective experts in the higher professional institutions.

Originality. The notion of "safe information and education environment in the higher educational institution" is specified. It is understood as information and education environment supplemented with hardware tools, software and managerial tools, safety devices ensuring protection against the negative information and personal information security of all the participants of the educational process in order to create adequate development conditions for the realization of their individual abilities and possibilities. The treats, model, principles, subsystems and components of a safe information and education environment organization, providing an effective systematic approach as a foundation of the educational process in professional training of to-be specialists are defined.

Practical value. Formulated regulations and practical recommendations for organization of safe information and education environment in higher educational institutions can be used in the educational process of higher education and in the system of advanced training (retraining) of educators.

Keywords: *safe information and education environment, informatization of education, information security (data security), professional educational institutions, professional training, system approach, information security threats*

Introduction. The present historical period is characterized by considerable transformations in the sphere of education, which are due to the influence of globalization processes, wide adoption of information processes and technology, information openness of the society. Competition in the sphere of education leads to the constant improvement of forms and techniques of education, to the creation of new educational technologies and means.

One of the characteristic tendencies of our time in the sphere of education is the creation and active use of the so-called information and education environment (IEE).

The content of this notion has been formulated in the governing documents of the Board of Education and Science. In the latest documents of the Board it is

pointed out that "there should be created conditions for the functioning of the electronic information and education environment which includes electronic information and electronic educational resources, the complex of information technologies, telecommunication technologies, technological means which in complex will provide the complete mastering of the curriculum of educational institutions including different forms of distant learning through information and communication technologies by the students regardless of the students' location".

Along with such advantages of the IEE as wide access to the educational content at any time, from anywhere, individualized instruction and monitoring, rapid spread of the best educational practices, it should be noted that the problem of information security remains topical not only for the participants of the educational process, but for the institution itself. We believe that both the nature of the problem and possible ways of its solution lie at the intersection of such disciplines as pedagogy, psychology, computer science, ergonomics, systems theory, and others.

Thus, nowadays a unified comprehensive approach to secure information and education environment in a higher educational institution is required, which fully takes into account the new possibilities of creation, spread and application of multicomponent distributed and integrated education oriented databases and knowledge bases, taking into account the national requirements to the educational system and interaction with the world educational resources. Considering the complexity and multi-task organization of safe information and education environment in higher educational institutions, it is recommended to apply the systematic approach.

Analysis of the recent research. Ludwig von Bertalanffy is considered to be the founder of the systematic approach. A notable contribution to this field has been also made by E. de Bono, L. la Rush, Simon G., P. Drucker, A. Chandler. The leading representatives of the systematic approach in domestic science are I. V. Blauberg, D. M. Gvishiani, V. P. Kuzmin, V. A. Lektorsky, V. N. Sadovsky, A. I. Uyomov, I. T. Frolov, E. T. Yudin and others.

Information security issues in education were studied by such scholars as Polyakov V. P. [1] who dealt with the problem of information security and offered methodic system of teaching information security to students of technical colleges, and Grachev G. V. dealing with the problems of the information psychological security of individuals as well as a number of others.

A series of works dedicated to the engineering aspects of information security are also known [2–4]. These works deal with the protection of information, the choice of the technical means of information protection, building-up of corporate information security systems.

Presentation of the main research. The precondition for the creation of the IEE is based on the achievements in the field of information technologies and accumulated experience of their application in the educational process. Computer equipment and data transmission have gone a long way from unsystematic, haphazard application to a widespread use. There is currently a process of changing them into a new quality – the development and functioning of the information and education environment, which together with the hardware, software, and information component includes methodological support.

A landmark event in the development and application of the IEE stemmed from the wide use of personal computers and from facilitated access to the global network Internet. These above mentioned factors have made it possible to identify and implement new teaching resources, which occurred due to the simplicity of the dialogue communication, prompt access to global information resources, a quick search of necessary information, and the ability to visualize the educational material. There appeared such notions as a "virtual laboratory", "virtual tour", "virtual classroom", "virtual campus", "virtual university" and others. All of them, in our opinion, may be included in the concept of information and education environment.

Modern IEE of the higher educational institution ensures the implementation of the process of professional and personal self-development of a to-be specialist, i.e. allows independent choice of individual educational trajectory, forms and methods of solving professional problems, methods of monitoring, reflection and self-evaluation of the educational activities of students. It offers individual choice of subjects, creative laboratories and other types of classes which are defined in the basic curriculum as electives; it advances and deepens the content of educational material; individual choice of subjects and more creative work on the subject; the right to an individual picture of the world and reasonable positions for each educational area. It also gives an opportunity to study the material more quickly and more thoroughly, to choose individually additional topics for project and creative work in subjects, to form the individual world view and motivated position in every sphere.

Analysis of the IEE of a higher educational institution indicates that it should provide: an access to the curricula, working programs of educational disciplines (modules), to the programs of practices, to publications in electronic library systems and electronic educational resources specified in the working programs:

- the educational process record, the record of the results of interim assessment, and the results of mastering training programs;
- carrying out all kinds of activities, procedures of assessment of learning outcomes, in other words educational evaluation whose implementation is provided through the use of e-learning, distance learning technologies;
- formation of students' electronic portfolios, including the preservation of the student's works, reviews and evaluations of these works by the relevant participants in the educational process; the interaction between the participants of the educational process,

including synchronous and (or) asynchronous communication via the Internet, etc.

The functioning of the electronic information and education environment of the higher educational institution is provided by adequate means of information and telecommunication technologies and by skilled specialists, operating and maintaining it.

The material basis of the IEE is based on a set of computer equipment, software, data transmission channels, display and information storage means widely used in the educational process. In addition, the students themselves actively use mobile phones, smartphones, pocket PCs, as useful tools helping to store, look through the information and to communicate.

It is obvious that the IEE of the higher educational institution is a member of the global information and education space, in which different participants interact. These participants are students, teachers, administration, network administrators, on the one hand, and educational, social and other organizations, on the other hand. The development of the IEE is a highly knowledge-based activity, which involves the work of co-educators, psychologists, methodologists, programmers and computer designers.

Thus, on the one hand, it can be stated that the IEE of the higher educational institution today is quite a developed system; on the other hand, one cannot ignore the fact that unrestricted access to the information content has certain risks and threats both for the individual learners and tutors, and for the corporate interests of the educational organization.

The experience of high educational institutions shows that the problem of security of the IEE is primarily determined by the information security and, therefore, one of the aims during its design and construction should be the aim of implementing information security requirements.

By the safe information and education environment (BIOS) of the higher educational institution we will mean the information and education environment of a higher educational institution, supplied with hardware, software and organizational means and methods of protection against the negative information, which provides security and protection of personal information among all the participants of the educational process at the university in order to create conditions for the most full-value development and implementation of their individual abilities and capabilities [5].

The organization of BIOS of the university should be preceded by the analysis of possible sources of information security threats and their nature in the educational organization. The nature of the information threats is connected with the character of a modern university providing access to the IEE to different groups of users. The university IEE may have different categories of users whose requirements for information security differ. They are the university students studying in various forms, professional and teaching staff and the administration, the school children as the participants of preparatory training courses, the students enrolled in various training courses and extension courses as well as representatives of organizations cooperating with the university, such as research and development (R&D).

Obviously, the main group of potential perpetrators of information security for the IEE are students who have a sufficiently high level of professional IT-training. Characteristic age features of their psyche cause them to commit illegal acts aimed at violating information security (for example, to block access to the site of the university, to get the right to view and edit public information, etc.).

Information security vulnerability of the higher institution is also determined by the multifaceted nature of its operations, the variety of information flows, including the outer space and the information coming out from it, by territorial distribution of its infrastructure (providing divisions, branches, representative offices).

The following information security threats are essential for the educational institution:

- violation of confidentiality (unauthorized data accessing, including personal data of teachers and students, service information about the university);
- technical failures and malfunctions of computation and data communication equipment, energy supply equipment violations, physical destruction or damage of equipment, etc.;
- malicious and troublesome software, hacker attacks and spam; unauthorized use of unlicensed software;
- copyright and intellectual property infringement, etc.

At the same time, the so-called personality information threats, defined as a set of conditions and factors that endanger the vital interests of the individual are common for students, teachers and university staff; they include: adherence to and implementation of the constitutional right to seek, receive, produce and transmit information; citizens' rights to privacy; the use of information for the spiritual, physical, intellectual development; protection of intellectual property; ensuring the rights of citizens to protect their health from the unconscious harmful information [6].

The information threats directed against the person can also include the criminalization of the information space (illegal content, cyber cheating); threats from the dataflow; the threat of negative impact on the health and psyche of the person, addiction to the network and computer games, the student's personality blur, threat of violation of an author's rights.

In general, information threats are determined by violation of the conditions of confidentiality, integrity and availability of the information in the IEE.

Thus, the provision of safe IEE of the higher educational institution is a complex multifaceted problem. To solve it a systematic approach should be applied which involves consideration of the IEE as a complex system and the gradual transition from the general to the particular. While the goal is the basis for the examination and the object under study is singled out of the environment.

In our opinion, such an approach should be based on the application of a number of principles: i.e. the systemacity principle, the hierarchical pattern of cognition, the principle of integrity, the principle of formalization.

The systemacity principle means that the IEE is considered as a system, i.e. all the connections with the environment are taken into consideration, as well as the possibility of division into elements, taking into account the backbone links.

Figure shows that the IEE of the higher educational institution operates in the global information and education environment, interacting with IEEs of other educational, scientific and other organizations.

As an example, the domestic Internet University of Information Technologies (http://www.intuit.ru) can be mentioned which offers both a lot of free training courses for users of the global Internet and an opportunity to receive the second higher education on a commercial basis (full-time with the intramural tests and examinations); its database has about half a million users. Within the framework of the Global Alliance of the UN Information and Communication Technologies and Development (GAID) there operates a non-profit online higher educational institution – University of the People (http://uopeople.edu/), in which it is planned to train 15 thousand people at a time.

When applying the systematic approach to BIOS of the higher educational institution decomposition (structuring) should be carried out taking into account the objectives of the structural research – identifying the elements which affect the security of the system, their relationships and interaction. Obviously, the centres of storing information, data channels, access points to information resources, users of IEEs and other things can be represented as such elements. Their common feature is their hierarchical nature, both of the decomposition and the structure formed as a result of its implementation.

Thus, while organizing the safe IEE of the higher educational institution from the point of view of its functional components, some isolated subsystems can be singled out: learning content, teaching materials, management documentation, local legal acts, financial documents, and a number of others.

Regarding the support of safe operation of the IEE, the following subsystems can be singled out: technical (hardware), software, information, mathematical, organizational and staffing.

Further decomposition of, for example, logistics subsystem, leads to differentiation of a plurality of computers belonging to a computer network. Each computer can be presented as part of the IEE, on the one hand, and as a system that includes the individual devices as its elements, on the other hand.

The issue being analysed from the perspective of secure communication between the elements and subsystems in the real IEE of the higher educational institution, it should be noted that the number of all the relationships is huge, so it is impossible to explore everything, and it is necessary to limit their number artificially, i.e. the links that do not affect the safety are irrelevant and can fail to be viewed.

According to the principle of hierarchy of cognition, the IEE of the higher educational institution requires three-level study of IEE: the study of the subject – "the proper level", the study of the same subject as part of a wider system – "a higher level", and finally, the study of this subject in relation to the constituents of the subject components – "the lower level". This bi-directional information flows are analysed as well as potential actions with the upstream and downstream levels. The higher level for the IEE is a global information and education environment based on the Internet (Figure).

The lower level is formed by the above-mentioned subsystems and the elements of the IEE. This suggests that while organizing secure IEE one should analyse both possible information security threats either "from above", such as hacker attacks on the university website and actions aimed at violation of information security or "from below", i.e. by the staff and students of the university.

The principle of integrity reflects the peculiarity of the systematic approach, it aims to explore integrative properties and regularities of the IEE of the higher educational institution, i.e. these properties are inherent in the system as a whole, but do not occur in the aggregate of its component elements. Therefore, the BIOS of the educational institution as a system has a new quality – it creates a set of conditions under which educational and professional work of students and teachers directly develops, the personal qualities of students are formed, the management and methodological activities are provided, the competence of the information security of the person is formed.

The principle of formalization of BIOS consideration as a system means that a systematic approach is aimed at obtaining quantitative characteristics to provide a secure environment protection, development of methods, narrowing the ambiguity of concepts. Speaking of the IEE of the higher educational institution viewed systematically, it is necessary to give substance to such concepts as efficacy, safety and quality, to build a model of a safe educational environment.

Since the main task of the university is professional training, it is obvious that a safe IEE contributes to its fulfilment, realizing the providing function. Therefore, when evaluating the key effectiveness indicators and the quality of training graduates, it is necessary to consider the impact of the information security factor on the final outcome. The application of the systematic approach to the organization of safe IEE of the higher educational institution has four basic steps:

- clarification and goal-setting arrangements for the safe IEE of the higher educational institution;
- BIOS model building that meets the objectives of the organization for the secure IEE of the higher educational institution;
- carrying out experiments with the model;
- processing and interpretation of the results, the application of them into the system.

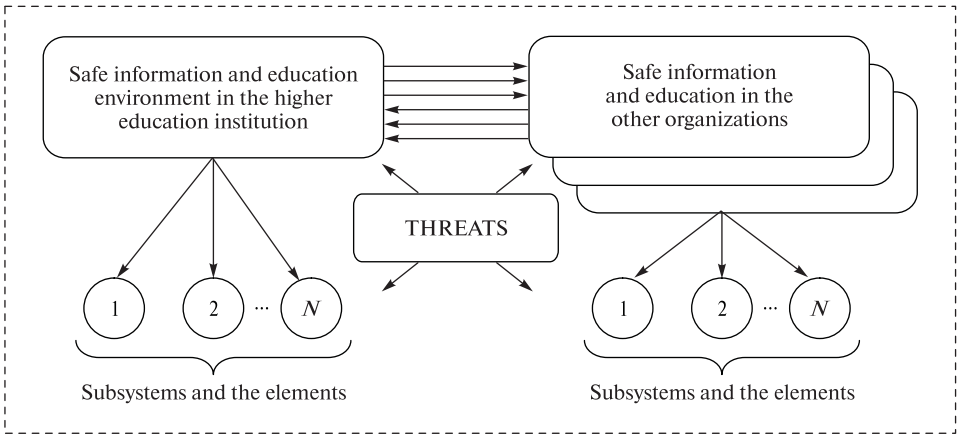

Fig. The systemic nature of the information-education environment of the higher educational institution

Building of a model of the safe educational environment of the higher educational institution involves the following steps: selection of (the formation of) quality and efficiency features of the system and their rationale; description of the system; model validation and substantiation of its adequacy. The choice (formation) and substantiation of the quality and efficiency features are based on the analysis of the objectives of the system (subsystems), tasks and objectives of the research.

Systematic description of the IEE of the higher educational institution should reflect the functional properties of the system (the contents of activity and operation), morphology (components and relationships between them), information features (accuracy, organization, uncertainty, handling, etc.). In accordance with this description, the IEE as a system may be functional, morphological and informational.

Functional description of the BIOS of the higher educational institution is carried out on the basis of the performance indicator, reflects the processes occurring in the system, and the nature of the operation. It should cover the processes occurring in the system when it is used, and to show a method for producing the output features of the system (efficiency) in a particular situation or a group of situations. The mathematical apparatus of the functional description of the BIOS in the higher educational institution must meet two requirements: the adequacy of the task and its capability to perform calculations.

Functional description should reflect the following aspects inherent in the BIOS: professional, organizational and interpersonal ones [5].

The BIOS subsystems can be singled out into the following groups:

- the subjects of the educational process (students, teachers, university entrants, assisting personnel, invited experts);
- the educational process (goal, stages, content, forms, methods);
- provision of the educational process (legal, personnel, scientific-methodical, informational, organizational, material, financial, motivational);
- external relations (in the external educational environment, in the society, in various fields of activities related to the areas of training of specialists).

Interaction of the components and subsystems of the BIOS generates the pedagogical process. In other words, it is created and functions in order to ensure optimal flow of the pedagogical process with the aim of training professionals.

From this point of view, we can provide the following set of BIOS functions of the higher educational institution:

- scientific and methodological support of educational activities in the higher educational institution (working-out, storage and use of teaching materials, texts of lectures, laboratory work description, etc.);
- interactive support of the educational process with the inclusion of imaging (visualization);
- ensuring the control of students' knowledge, built on an intelligent test system;
- organization of the work of virtual laboratories and hypermedia of educational space;
- informational support of students' projects and diploma theses;
- maintenance of information - a reference database (full-text library, access to e-library systems, dictionaries, glossaries);
- organization of distance learning;
- organization of virtual communication between the participants of the educational space, accumulation and spread of teaching experience, professional development (refresher training) of teachers;
- public relations, formation of positive image of the higher educational institution;
- security provision, primarily – informational security.

The starting point of the functional description is to constitute a link between the effectiveness of the BIOS as a system and its operation conditions (properties of the situation). The main purpose of the BIOS as a secure informational environment of students and teachers at the same time is not necessarily used (it should be included in the functional description a little

later), so in most cases one may find the model forms and schemes of descriptions useful.

The most common of them is the following. A list (set) of features characterizing the situation with the indispensable achievement of established safety parameters and the desired results of the system (its purpose) is made. This set of features is ordered and considered as a functional space, that is, a common language to describe the system is introduced. We introduce the basis (numeric or logical), and the metric topology. The resulting metric space is considered as a functional space BIOS of the higher educational institution. The functional educational environment of the higher educational institution that meets the safety requirements is constructed in this space.

The initial set of features may include the following subsets:

- continuously measurable features (tuition fees, the number of connections to information and educational resources of the university, the number of unauthorized attempts to access the information system of the university, etc.);
- discretely measurable features (indicators of the quality of education, the number of students, the number of professors and teaching staff, information on training equipment, etc.);
- ordered features (the location of the subjects on the scale of achievement, academic ranking, the age of teachers, etc.);
- disordered features ("have been accredited", "licensed", "information security threats", etc.);
- nebular features (disordered, uncertain, vague: "convenient", "visual", "promising", "familiar").

Metrication of the functional space of the higher educational institution BIOS, built on such diverse features suggests certain difficulties which can be overcome by the factorization, i.e., by highlighting the main defining features and the introduction of the basis. The starting point of the functional description is the functional performance criteria.

Morphological description of the BIOS as a system is preceded by the decomposition of the system, which can be carried out in various ways. As an example, let us consider two methods of decomposition of the IEE of the higher educational institution. Let there be an IEE of the higher educational institution equal to S, decomposition of which can be performed by functional feature, for example, as follows

$$S = S_1 US_2 US_3,$$

where S_1 is an organizational management subsystem; S_2 is a training subsystem; S_3 is a management subsystem of research activities of students and teachers. Then organizational management subsystem can be represented as

$$S_1 = S_{11} US_{12} US_{13} US_{14},$$

where S_{11} is a management subsystem; S_{12} is a financial subsystem; S_{13} is a subsystem of safety management; S_{14} is a subsystem of management of economic activities.

Training Subsystem

$$S_2 = S_{21} US_{22} US_{23},$$

where S_{21} is learning content management subsystem; S_{22} is a subsystem of management and organization of the educational process, S_{23} is a subsystem of informational security.

Further, a security management subsystem can be represented as

$$S_{13} = S_{131} US_{132},$$

where S_{131} is a subsystem of informational security; S_{132} is a campus security subsystem.

Hereafter, the decomposition can be continued, and S_{21}, S_{22} may also include administering, controlling and conclusive subsystems on their own level.

On the whole

$$S = US_{ijk} \ldots m;$$

$$i = 1, \ldots, i_0; j = 1, \ldots, j_0; k = 1, \ldots, k_0, \ldots; m = 1, \ldots, m_0,$$

where i_0 is the number of subsystems of the first level, j_0 is the number of subsystems of the second level, etc.

Another option of (binary) BIOS decomposition of the higher educational institution is that each subsystem is divided into two subsystems, the management subsystem and educational subsystem

$$S = S_1 US_2;$$

$$S_1 = S_{11} US_{12}; \qquad S_2 = S_{21} US_{22};$$

$$S_{21} = S_{211} US_{212} \ldots$$

Morphological description of the BIOS as a system is a diagram (graph) or a set operation. The decomposition is performed according to a plan of the system development, starting from the basic idea and hypotheses on its implementation. After the decomposition, the combining of subsystems with the help of direct and inverse backbone links (information, management and others.) is carried out.

Informational description is connected with the external and internal information exchange and reflects the uncertainty of the system. Informational description in the most general form, can be represented by the entropy of the system

$$H = -\int p(x) \log_2 p(x) dx$$

or

$$H = \sum p_i(x) \log_2 p_i(x),$$

where $p(x)$, $p_i(x)$ are continuous and discrete probability distribution of some x parameter characterizing the BIOS of the higher educational institution, for example, the probability of confidentiality breach.

From the informational entropy one can proceed to the errors in the assessment of the system, such as unauthorized access to personal data, the probability of the access to confidential information, the probability of the decommissioning of informational support

for the successful hacker attacks on the IEE of the higher educational institution.

Data description consists of a set of parameters $x_1(S_{ijk}...m)$, characterizing each subsystem, the laws of their distribution $p_1(x_1)$ (or the points of distribution in the corresponding approximation) and entropy values $H_1(S_{ijk}...m)$. The total entropy of the system is

$$H_\Sigma(S) = \sum_{i=1}^{L} H_l(S_{ijk...m}),$$

where L is the number of subsystems of the BIOS.

In the beginning, the descriptions may mutually disagree, but the comparison of descriptions opens the way to reducing uncertainty, encouraging obtaining the new data in order to identify the areas of risk and to clarify the descriptions on the basis of new data. In the end, all the descriptions are so coordinated that they can be combined to make a constructive description of the system, which will reflect the morphological, informational, functional features and the relationship between them. Initial descriptions are based on the ideas for informational security of the IEE of the higher educational institution, constructive description encourages the development of the ideas and proposing the new ones.

Thus, the systematic approach to the study of the safety of information and educational environment of the higher educational institution allows outlining a simple scheme of study and taking into account all the factors affecting the operation and efficiency of such systems, as well as formulating "practical recommendations on the organization of a safe educational environment in the higher educational institution" which may include, for example, the following measures:

1. Determination of the nature and classification of potential informational threats to the students, faculty, university administration.

2. Formation of the action plan for the organization of a safe educational environment in the higher educational institution to meet the requirements of the national and international legislation, to define the circle of responsible departments and individuals.

3. Development and implementation of the informational security policy and technical and organizational requirements by all the participants of the educational process. The development of regulations to ensure the full protection of both the information itself and individual students and teachers.

4. Continuous monitoring of the functioning of the BIOS, the identification of new threats, analysis of proposals and recommendations for further modernization of the BIOS.

It is obvious that the process of organizing a safe educational environment is continuous and cyclic. In the process of the IEE operation it is necessary to return to the first step, which entails repeated subsequent phases. Thus, the IEE will be modified to perform its tasks effectively at the same time ensuring informational security.

Conclusions. From the above-stated facts it can be concluded that the organization and functioning of a safe educational environment of the higher educational institution is impossible without the systematic approach, in which each component is a relatively independent subsystem and has a number of elements.

The information and education environment projected on this basis can, in our opinion, provide comfortable conditions for the comprehensive activities of the higher educational institution, it can meet the requirements for the training of students, and on the whole solve the problems associated with the prevention of possible negative physical and mental health consequences which can occur due to the information and emotional intensity of the subject environment.

References/Список літератури

1. Polyakov, V. P., 2006. *Methodical system of training of information security university students*. DEd. N. Novgorod.

Поляков В. П. Методическая система обучения информационной безопасности студентов вузов: автореф. дис. на соиск. научн. степ. д-ра пед. наук / Поляков В. П. – Н. Новгород, 2006. – 47 с.

2. Andrianov, V. V., Zefirov, S. L., Golovanov, V. B. and Golduev, N. A., 2011. *Obespecheniie informatsionnoi bezopasnosti biznesa* [Providing business information security], Alpina Publishers.

Обеспечение информационной безопасности бизнеса / Андрианов В. В., Зефиров С. Л., Голованов В. Б., Голдуев Н. А. // Альпина Паблишерз. – 2011. – 338 с.

3. Petrenko, S. A. and Kurbatov, V. A., 2011. *Politiki bezopasnosti kompanii pri rabote v internet* [Company security policy when using the Internet]. DMK Press.

Петренко С. А. Политики безопасности компании при работе в интернет / Петренко С. А., Курбатов В. А. // ДМК Пресс. – 2011. – 396 с.

4. Alan G. Konheim, 2007. *Computer security and cryptography*. John Wiley & Sons, Inc.

5. Korotenkov, Yu. G., 2011. *Informatsionnaia obrazovatelnaia sreda osnovnoi shkoly* [Information educational environment of primary school]. Akademiya IT.

Коротенков Ю. Г. Информационная образовательная среда основной школы / Коротенков Ю. Г. – М.: Академия АйТи, 2011. – 152 с.

6. Privalov, A. N. and Bogatireva, Yu. I., 2012. The main threats to information security subjects of the educational process. *News of the Tula State University. Humanitarian sciences,* No. 3, pp. 427–431.

Привалов А. Н. Основные угрозы информационной безопасности субъектов образовательного процесса /А. Н. Привалов, Ю. И. Богатырева // Известия Тульского государственного университета. Гуманитарные науки. – 2012. – Вып. 3. – С. 427–431.

7. Bogatireva, Yu. I., Privalov, A. N. and Romanov, V. A., 2014. Info safe environment of the school as a condition of the information security of the younger generation. *Informatics and Education*, No. 9, pp. 84–89.

Богатырева Ю. И. Инфобезопасная среда школы как условие обеспечения информационной бе-

зопасности подрастающего поколения / А. Н. Привалов, Ю. И. Богатырева, В. А. Романов // Информатика и образование. – 2014. – № 9. – С. 84–89.
8. Fedorov, V. A. and Davydova, N.N., 2014. Control of the research and education network development in modern socio-pedagogical conditions. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universitetu*, No. 2, pp. 126–132.

Федоров В. А. Управление развитием научно-образовательной сети в современных социально-педагогических условиях / В. А. Федоров, Н. Н. Давыдова // Науковий вісник Національного гірничого університету. – 2014. – № 2 (140). – С. 126–132.

Мета. Організація безпечного інформаційно-освітнього середовища ВНЗ шляхом застосування системного підходу.

Методика. Вивчення та науково-теоретичний аналіз літератури з досліджуваної проблеми, праксиметрический метод, моделювання, дослідження й узагальнення ефективного досвіду застосування системного підходу в освітніх професійних організаціях.

Результати. Створення безпечного інформаційного середовища в освітній професійній організації є необхідною умовою забезпечення комфортної професійної підготовки майбутніх фахівців у ВНЗ.

Наукова новизна. Уточнено поняття „безпечне інформаційно-освітнє середовище ВНЗ", що розуміється як інформаційно-освітнє середовище, доповнене апаратними, програмними та організаційними засобами, способами захисту від негативної інформації, що забезпечує безпеку й захист приватного інформаційного середовища всіх суб'єктів освітнього процесу з метою створення умов для повноцінного розвитку та реалізації їх індивідуальних здібностей і можливостей. Визначені: загрози, модель, принципи, підсистеми та елементи організації безпечного інформаційно-освітнього середовища, що забезпечують ефективність системного підходу як основи конструювання навчального процесу у професійній підготовці майбутніх фахівців.

Практична значимість. Сформульовані положення та практичні рекомендації для організації безпечного інформаційно-освітнього середовища у ВНЗ можуть бути використані в освітньому процесі ВНЗ і в системі підвищення кваліфікації (професійної перепідготовки) працівників освіти.

Ключові слова: *безпечне інформаційно-освітнє середовище, інформатизація освіти, інформаційна безпека, освітні професійні організації, професійна освіта, системний підхід, загрози інформаційній безпеці*

Цель. Организация безопасной информационно-образовательной среды ВУЗа путем применение системного подхода.

Методика. Изучение и научно-теоретический анализ литературы по исследуемой проблеме, праксиметрический метод, моделирование, исследование и обобщение эффективного опыта применения системного подхода в образовательных профессиональных организациях.

Результаты. Создание безопасной информационной среды в образовательной профессиональной организации является необходимым условием обеспечения комфортной профессиональной подготовки будущих специалистов в ВУЗе.

Научная новизна. Уточнено понятие „безопасная информационно-образовательная среда ВУЗа", понимаемая как информационно-образовательная среда, дополненная аппаратными, программными и организационными средствами, способами защиты от негативной информации, которая обеспечивает безопасность и защиту личной информационной среды всех субъектов образовательного процесса в целях создания условий для полноценного развития и реализации их индивидуальных способностей и возможностей. Определены: угрозы, модель, принципы, подсистемы и элементы организации безопасной информационно-образовательной среды, обеспечивающие эффективность системного подхода как основы конструирования учебного процесса в профессиональной подготовке будущих специалистов.

Практическая значимость. Сформулированные положения и практические рекомендации для организации безопасной информационно-образовательной среды в ВУЗе могут быть использованы в образовательном процессе ВУЗа и в системе повышения квалификации (профессиональной переподготовки) работников образования.

Ключевые слова: *безопасная информационно-образовательная среда, информатизация образования, информационная безопасность, образовательные профессиональные организации, профессиональное образование, системный подход, угрозы информационной безопасности*

Рекомендовано до публікації докт. техн. наук С. І. Логвиновим. Дата надходження рукопису 22.08.15.