Е. Н. Бояров, С. В. АБРАМОВА, П. В. СТАНКЕВИЧ, И. В. КОРНЕЕВА

Анализ информационных рисков в образовательной среде

Введение. Актуальность проблемы цифровизации образования связана с информационными трансформациями, происходящими в мире, а также тенденцией использования онлайн-технологий. Очевидно, что в условиях вынужденной информационной изоляции удаленный доступ к образовательным ресурсам востребован как никогда. С одной стороны, это влечет за собой резкое повышение значения информационных и цифровых ресурсов в образовании. Но, с другой стороны, это приводит к появлению широкого спектра угроз и опасностей, которые определяют риски как для существующих информационных систем в образовании, так и для новых.

Целью исследования является выявление факторов риска информации в современной образовательной среде, на основе которых можно проводить вероятностный анализ ее защищенности.

Материалы и методы. Методологической основой исследования послужили теория и практика информационного и системного подходов; моделирование вероятностной модели информационных рисков на основе сценариев.

Результаты и обсуждение. Исследование информационного аспекта безопасности образования показало, что существует довольно значительное количество рисков для информационных систем в образовании. При этом спектр таких рисков непрерывно расширяется ввиду специфики самих информационных процессов в образовании. Это требует учета таких рисков и принятие на системной основе мер по их оценки в контексте соотнесения дефиниций «актив», «уязвимость», «угроза» и «ущерб» в информационной образовательной среде. Соответственно такой, основанный на сценариях подход, позволяет создать общую схему «политики безопасности» в отношении информационных рисков в образовании. Его реализация представляет собой управление рисками, основанное на анализе причин и последствий нарушения ИБ, что также позволяет проводить регулярный анализ безопасности всей информационной образовательной среды.

Выводы. Разработанный метод оценки рисков информационной безопасности позволяет оценить существующий уровень риска и проводить регулярный анализ безопасности для всей образовательной среды на основе вероятностной модели, построенной на основе сценарного метода оценки информационных рисков образовательной среды

Ключевые слова: информационная безопасность, информационный риск, цифровизация образования, метод оценки рисков

Ссылка для цитирования:

Бояров Е. Н., Абрамова С. В., Станкевич П. В., Корнеева И. В. Анализ информационных рисков в образовательной среде // Перспективы науки и образования. 2021. № 3 (51). С. 451-464. doi: 10.32744/pse.2021.3.32

E. N. BOYAROV, S. V. ABRAMOVA, P. V. STANKEVICH, I. V. KORNEEVA

Analysis of information risks in education

Relevance. Digitalization of education is becoming an increasingly urgent issue today. This is due both to the information transformations taking place all over the world and the online technologies usage trend.

The education system as an integral and determinative part of all processes in society is also under the influence of the trend. It is obvious that under the conditions of informational isolation, remote access to educational resources is in demand more than ever.

On the one hand, it entails a sharp increase of the importance of information and digital resources in education. But on the other hand, this leads to the wide range of threats and dangers that determine the risks for existing information systems in education and new ones.

The aim of the study is to identify the information risk factors in the modern educational environment, on the basis of which it is possible to carry out a probabilistic analysis of its security.

The methodological basis of the research combines the theory and practice of information and system approaches; modeling of a probabilistic model of information risks based on scenarios.

Results and discussion. The study of the information aspect of education security has shown a fairly significant number of risks for information systems in education.

At the same time, the range of such risks is constantly expanding due to the specifics of the information processes in education.

It requires to take into account such risks and to assume system based measures aimed to assess the risks in the context of correlating the definitions "asset", "vulnerability", "threat" and "damage" in the information educational environment.

Accordingly, this scenario-based approach makes it possible to create a general scheme of "security policy" in relation to information risks in education.

Its implementation is represented as a risk management based on the analysis of the causes and consequences of an IS violation that also allows to analyze the security of the entire information educational environment.

Conclusion. Implementation of the developed method allows to assess existing levels of risk and to conduct regular security analysis for the entire educational environment on the basis of probabilistic model based on the scenario method of educational environment information risks assessment.

Keywords: information security, information risk, digitalization of education, risk assessment method

For Reference:

Boyarov, E. N., Abramova, S. V., Stankevich, P. V., & Korneeva, I. V. (2021). Analysis of information risks in education. *Perspektivy nauki i obrazovaniya – Perspectives of Science and Education*, 51 (3), 451-464. doi: 10.32744/pse.2021.3.32

Introduction

When people use the Internet to search for some information, they are permanently at risk of encountering misinformation. Information seekers deal with this threat by evaluating the credibility of the provided information and the trustworthiness of the information source. To make such evaluations, information seekers ask themselves whether the information source is an expert in his field and whether the information source bases his argumentation on scientific studies.

Given the danger of potential misinformation, seekers of some information (information about educational or other) have to decide whether they should accept knowledge claims they encounter online. According to the Content-Source Integration Model [30], information seekers can and do use first-hand and second-hand evaluations to make such decisions. First-hand evaluations can be understood as answers to the question “Is this statement/claim true?”. To answer this question, information seekers can compare whether an encountered knowledge claim is compatible with their own prior knowledge on the topic and evaluate the knowledge claim’s logical coherence. However, making first-hand evaluations is often difficult for information seekers when they encounter scientific information, because scientific knowledge claims can be highly complex and specialized due to the division of cognitive labor in modern societies.

Risk perception is commonly defined as “the subjective judgment that people make about the characteristics and severity of risk” [27, p. 8] in reference to judgments or arguments. Risk perception affects the personal decision-making process based on an individual’s frame of reference and is developed over a lifetime [8]. Although participants in the educational process commonly experience inaccurate or incorrect information, risk perception of the disaster varies by individuals’ psychological frames and/or previous experiences and reflects specific individual values. From the cultural theory perspective, risk perception is viewed within the social contexts in which an individual finds her/himself [28].

Information-seeking efficacy is defined as an individual’s confidence in seeking necessary information to overcome difficult situations or to resolve problems [10]. It is a type of self-efficacy within the context of information.

While analyzing research works devoted to IS problems it can be noted that, in essence, the concept of “information security” finds various interpretations. This, in particular, is associated with a significant number of various aspects of IS. In addition, it correlates with the understanding of information in terms of its availability [31].

At the same time, the authors classify aspects of IS giving their own definitions for the term. In addition, research works on defining IS standards can be classified to the given category.

The vast majority of research works in the field of IS belongs to the first category. The disadvantage of this approach is the impossibility to connect all existing cause-and-effect relationships influence on a specific aspect of IS&IR during the study.

The prerequisites for setting the problem of IS&IR identification in educational process is the trend of digitalization in all spheres of human economic activity and in the education system as a part of it.

Literature review

Researchers have noted that digitalization in Higher Education institutions is an issue that concerns many educational stakeholders [4; 7]; digital technologies are currently one of the most used resources among students for developing their personalized learning environment [23]. They find that digital technology has become a central aspect of higher education, inherently affecting all aspects of the student experience. It has also been linked to an increase in behavioral, affective and cognitive student engagement, the facilitation of which is a central concern of educators [5; 6]. Other researches consider thanks to the globalization of e-learning practices, these educational experiences can be made available to students from different geographical regions and universities, which promotes the development of international and inter-university cooperation in education [11].

Thus, digitalization is caused by a significant increase in the volume of information as the main branch resource (for example, in education sphere). It also determines the need for innovative solutions that can be found through digital transformation. They can lead to the optimization of educational and management processes, cost reduction (for example, reducing teachers' workload) and the emergence of new sources of branch income (for example, the organization of a distance learning courses, the development of digital educational resources, etc.).

IS problems can be considered as another «point de repère» that can be explained by the following positions of the authors. Since most of the Internet is not governed by editors, the validity of online information cannot be guaranteed. Therefore, information seekers have to decide whether they should accept knowledge claims they encounter online [18].

So the necessity to take into account all information risks of modern education is becoming more obvious today. And researchers are increasingly paying attention to this issue.

They develop a risk assessment model that supports companies in the investment decision-making process regarding IT security measures by identifying and evaluating the most critical areas of the information network while considering the underlying production network. For this purpose, IT availability risks are quantified by means of graph theory, matrix notation, and value-at-risk. This model provides a structured approach and considers network structures and interdependencies [13].

In addition, security testing on risk analysis using STRIDE approach has been taken as a proposal to reduce the test suite size and to test the most vulnerable states in a system by using risk metrics [25] and some models use for activities of the project [20; 22].

In some article protection of individual academic rights of students, including works: to protect against unreliable information. So, various approaches to understanding the essence of information audit, relationship of information audit and analysis of information risks are analyzed [32], challenges and risks associated with open education are identified [1; 17] and information risks in a post-industrial society are evaluated [21] in different scientific works.

Some studies are devoted to the risks of modern education in the context of personal IS [19], problems of ensuring IS for young people in the space of social networks [9], as well as IS&IR for schoolchildren [3].

Thus, the purpose of this work is to provide theoretical background for educational environment IS&IR scenario-based assessment method for assessment of IS&IR in educational environment.

This purpose has determined several problems that define the structure of this research work as following: Section 2. Security of education environment: informational aspect; Section 3. Adaptive capabilities of modern educational environment for reducing informational dangers; Section 4. Risks for information system in education; Section 5. Scenario-based IS&IR assessment method for the educational environment.

Materials and methods

1. Security of education environment: informational aspect

In the context of understanding the concept of “security” as the sense of protection of the vital interests of the individual, society and the state from internal and external threats, its essence in the pedagogical process is to protect the educational needs and interests of the participants (students and university teachers) in various fields of pedagogical activity from internal and external threats, ensuring the sustainability and quality of pedagogical education.

Analyzing various aspects of the safety of educational process (technical, psychological, pedagogical, environmental, health-preserving and others), it is worth to focus on the informational aspect.

The range of problems covering the issues of ensuring the IS&IR of the educational environment is widely represented in Russian and International studies (technologies for the secure storage, processing and use of information resources; protection of interaction means, devices for transmission and distribution of scientific and educational information etc.; directions of protecting students from negative information from the Mass Media and the Internet; informational and psychological issues of teaching.

The mentioned aspects within the educational environment are implemented through the following issues of IS such as legislative, organizational, engineering and technical ones.

The legislative direction of the security provision implies the development of regulatory documents, various regulations, rules, procedures and methodological guidelines to ensure the protection of the digital educational environment as a whole, information learning environment of educational organizations, and the personal information environment of all participants of the educational process.

The organizational direction includes the action plan for security and security measures to protect the critically important informational infrastructure of educational organization; work with pedagogical and support staff to identify potentially dangerous subjects of information influence; work with documents and information resources (both digital and traditional); activities to analyze and identify internal and external threats to the information educational environment.

The engineering and technical direction implies to use a set of physical means (including various means and structures that prevent the physical penetration of intruders into protected objects and storage media) to provide security to educational environment; hardware tools (including devices, gadgets and other technical means used to protect information from unauthorized negative impact); software (covering special programs, software systems and data protection systems in information systems and networks, as well as means of data accumulation and storage to ensure its actuality, integrity, availability and objectivity); cryptographic means (specialized mathematical and algorithmic means of information protection, intended for secure data link through telecommunication channels).

Equally important aspect of the educational process is the necessity to protect students from the information itself. We are talking about such properties of information as redundancy, reliability, relevance, adequacy, objectivity, integrity, completeness, etc. From these positions, it is necessary to ensure protection for participants of information interaction in the modern educational environment, by qualifying the following requirements for educational content:

- availability of the content of academic disciplines and modules, regardless of the students' location (at the lectures and practical classes or at home, including distance learning or in remote access under the conditions of self-isolation);
- relevance (timeliness) of educational content for a given time, under specific conditions (to explore the specific topic; in modern geoinformational conditions, etc.);
- clarity (understandability) of educational content for students (ability to change the level of complexity of educational material, control and measuring materials or tasks dynamically,);
- objectivity of the presentation of educational content based on the provisions qualifying the facts of real state of modern science, as well as the content of the material for an objective assessment of the quality of education and the competence of students;
- reliability of educational content, guaranteeing students to receive complete and reliable information about events, facts, phenomena, government regulations and requirements, etc.;
- differentiation of educational content that allows to provide students with conditions for the maximum development of his personal characteristics, satisfaction of cognitive needs and interests in the process of studying the educational content.

2. Adaptive learning

The idea of adaptive and personalized learning originated in the 1950s on the basis of the "learning machines" of B.F. Skinner, who created a mechanical box-like device that posed questions to students.

Correct answers were rewarded with new academic material; incorrect ones led to the repetition of the previous question.

According to B.F. Skinner's opinion, students learned quickly to give correct answers [29]. G. Pask assumes the presence of an adaptive mechanism for controlling the activity of the subject of learning, which maintains interest, attention and the rate of assimilation by presenting, solving rather difficult, but feasible tasks since knowledge and skills are mastered [26].

As shown by numerous author's studies, on the one hand, adaptive education adapts to the intellectual, emotional, evaluative and behavioral spheres of each participant in the pedagogical process. The defining feature of adaptive education is the development of a person's abilities for self-improvement based under his individual characteristics, abilities and interests. On the other hand, an adaptive educational environment should effectively adapt to changing conditions and factors, including factors that determine the security of the environment from the point of IS&IR.

The adaptive education system has been developed on the basis of recent trends in improving the educational process.

The adaptive variability of the educational information environment of an educational organization is based on the person-centered activity concept of education, which is focused on the student's personality, his emotional and social development.

At the same time, the student is considered as an individual who, firstly, can choose a path of learning to achieve the best results; secondly, teachers select methods and goal setting trying to adapt to the individual educational needs, abilities, capabilities and interests of each student through the wide use of project and thematic learning and interest-based learning; thirdly, as a subject of information interaction with an environment that has certain vulnerabilities.

Thus, the adaptability of information educational environment is manifested itself in adaptation to the individual qualities of the ability, the capabilities of each student under the mandatory requirement for safe interaction.

At the same time, such educational system is able, firstly, to help each student achieve the optimal level of intellectual development in accordance with his abilities, and secondly, to ensure safe communication in the information educational space. This allows us to determine a number of adaptive properties of such environment:

1) Adaptability to the requirements of each specific educational institution in terms of various parameters: the number of hours, professional orientation, quality of education providing the implementation of basic educational programs;

2) Adaptability to the forms of education providing the selection of education form that is most effective for this category of students, taking into account the proposed content of the main educational program.

At the same time, the combination of full-time, part-time and distance forms of study with mandatory remote support of the educational process (or with the use of blended form of learning) will take into account the peculiarities of building an individual educational route for a student (in combination of lectures and practical classes with individual work of students on program material with the possibility of distributed (remote) support);

3) Adaptability to the content of educational program (Principal Professional Educational Program) (variability), which allows students to individualize the learning process using variable modules (disciplines), that is especially important in a blended learning environment;

4) Adaptability to control the level of mastering of educational material, determining the presence of a variety of practice-oriented and multi-level tasks, selected according to the certain principle in the "case-tasks". The choice of these tasks depends not only on the decision of the teacher, but also on the decision of the students, who always have an opportunity to choose and go to a more interesting (meaningful) or a more difficult task;

5) Openness for modification of the components of secure information educational environment providing educational organizations to interact at the levels of information educational systems based on open interfaces regulated by publicly available regulations and technical documents, open standards and specifications with mandatory compliance for IS requirements;

6) Protection from the impact of negative external and internal factors in the information sphere due to adaptability to specific mechanisms of such threats. It becomes possible due to taking into account the specific scenario of information threats.

3. Risks of information systems in education

In some research papers, information risk is defined as a set of events that can affect information to one degree or another: distort or destroy, and negatively affect its confidentiality or availability which leads to the necessity of its identification and assessment [2], the choice of assessing model for permissible risk levels [14; 16], the determination of

the accuracy and completeness of risk factors' analysis and assessment [33], the critical reflection of problems and risks in education [35].

Others define the concept of information risk as a narrower aspect in computer system that cause hardware or software risks [23] and requires an audit of certain components in computer system [34].

Unfortunately, most of the author's concepts do not address some important aspects of IS & IR that are worth paying attention to.

But it is these data that will be the basis for constructing educational information both directly (the content of electronic textbooks, electronic lectures) and indirectly (while analyzing statistical data, the dynamics of the occurrence of dangerous events, incidents, etc.).

Also, this definition often does not include risks associated with the failures in information processing algorithms, programs that are used to implement the educational process (denial of access to educational material, incorrect sequence of educational material presentation, loss of a part or block of educational material, etc.).

Results

A recent study has found that all information risks in the educational environment can be classified into different groups based on several criteria:

1. According to sources, information risks are divided into internal ones, directly related to educational information, its physical carriers, participants of information educational activity (teachers, students, support personnel) and external risks related to external influence (destructive criminal influence on educational information systems, changes of external information background, etc.).

2. According to characteristics, risks are divided into intentional ones (associated with malicious actions both from the participants of information educational process and public at large, when the person knows about probably unfavorable outcome for information educational environment, but deliberately goes to it) and unintentional risks (realized due to the fact that the person does not assume under some factors (ignorance, incompetence, erroneous actions, etc.) that his actions may lead to risk);

3. According to types, risks can be divided into direct risks (associated with the educational process, its elements, content, objects and subjects of information educational process) or indirect ones (acting indirectly, since they are not directly related to the educational process);

4. According to results, there can be distortion, violation of the information actuality, violation of the relevance of information, violation of the completeness of information, violation of confidentiality of information, etc.

5. According to the mechanism of action, risks can be divided into objective risks (dangerous and emergency situations of various origins that led to the failure of the information educational system elements, with the consequences able to be assessed) and subjective ones (human errors of specialists serving the system, technological errors of system participants such as incorrect actions on interaction with electronic resources of various types, when consequences are difficult or almost impossible to assess).

Accordingly, information risk can be:

- accepted - accept the risk and incur losses caused by it;
- reduced - take a certain list of measures aimed to minimize the risk;

- transferred - to impose the costs for damage covering on the insurance company, or to transform the risk into a risk with a lower level of danger using special mechanisms.

In practice, there are several methodologies used for information risks assessment:

- CORAS (developed under the European program of Information Society Technologies. The essence of the methodology is to adapt, concretize and combine some methods of risk analysis, for example: - Event-Tree-Analysis, Markov chains and FMECA);

- OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation developed at the Institute of Software Engineering at Carnegie Mellon University to provide better involvement of the information owner in the identification of critical information assets and the risks. The OCTAVE method is a method of rapid assessment of critical threats, asset identification and vulnerability identification);

- Matrix Method of Analysis (connects assets, vulnerabilities, threats, controlling means and determines the importance of various controlling means in accordance with the assets of the organization. The assets of the organization are understood as significant objects that can be both tangible and intangible) [4; 24].

As noted in GOST ISO 15408 [12], the concept of “risk” is a consequence of the mutual relationship of the concepts of “asset”, “vulnerability”, “threat” and “damage”. Applying these definitions to information educational environment we should mention the following:

- Assets - key components of educational environment infrastructure and significant information (educational, personal, methodological, scientific, regulatory, etc.) processed in the informational education system;

- Threat – potential opportunity of damage causing by any previously known way;

- Vulnerability - weak point in the means of protection caused by errors or imperfections in procedures, projects and implementation the “threat” can overcome;

- Damage - costs for restoration of system to its initial condition (restoring the integrity, relevance, reliability of information significant for the educational process, etc.) after a potential IS incident.

Thus, risk means a combination of damage probability caused by the overcoming the protection system using vulnerabilities and the severity of this damage.

Risks are minimized by developing a behavior pattern called “security policy” (implemented as a model, method or scenarios) and by managing it (Fig. 1).

The management of the security policy implementation is the risk management based on the analysis of the reasons and consequences of IS violation.

Educational environment IS&IR assessment method based on scenario.

This method of assessment the IS&IR of the educational environment is based on the identification of its key asset, analysis of weaknesses in the protection system and strict supervision over them.

Thus, this method allows predicting of information risk scenarios for known vulnerabilities by analyzing the possibility of occurrence and realization of each information risk. It is implemented in a specific solution to reduce the identified risk. The risk assessment process is shown in Fig. 2:

The following sequence of actions is recommended to identify each risk and determine the level of its influence on the educational process:

Step 1: Determine the key asset of the information educational environment according to the classification of ISO / IEC 27005.

Step 2: Determine the vulnerabilities in the security system of information educational environment, including technically weak points and weaknesses in management.

Figure 1 Overall scheme of “security policy” for information risks in education

Figure 2 Process of scenario-based method for assessing the IS&IR of the educational environment

Step 3: Determine the severity level of the vulnerability. If the level of vulnerability is low it can be identified as an object of risk that must be monitored in order to identify its dynamics but if the level of vulnerability is high, it is necessary to build a risk scenario.

Step 4: Build a risk scenario.

Step 5: Assess the risk probability.

Step 6: Assess the impact caused by the risk (including informative, technical, technological, methodological, reputational impact and influence on the educational process).

Step 7: Determine the overall risk level of the educational information system.

Step 8: Develop the specific solution to reduce the risk assessment of IS in the educational environment.

The presented process has a system of direct and feedback links. On the one hand, they are necessary for making decision about the level of risk, and, on the other hand, to carry out iterations to assess the existing level of risk as fully as possible, as well as conduct a regular security analysis of the entire information educational environment.

Practical application of this model made it possible to identify the set of information security risks in the educational environment of universities (Table 1). The weight coefficients of specific risks were estimated by the team of geographically distributed independent experts.

Table 1

Parameters of the information risks' impact on the information-educational environment with weight coefficients

IR parameter (IRp)	IR type (t)	Weight coefficient (w)
Type of environment by level of protection (1)	Unprotected environment (no defense mechanisms available) (1)	10
	Environment with minimum safety (separate systems and means of information security) (2)	5
	Completely secure environment (secure protocols in use) (3)	2
Attack susceptibility (2)	Environment prone to more attacks (1)	10
	Environment prone to less number of attacks (2)	5
	Environment not prone to attacks (3)	2
The number of different educational systems and intermediate technologies involved and integrated into a single structure (3)	Various systems involved (information, technological, administrative, managerial, educational, etc.) (1)	10
	Some systems are involved in (2)	5
	No systems are involved in (3)	2
Security of the environment elements (4)	Completely unprotected elements (information networks, resources, equipment, etc.) (1)	10
	Partially protected elements (2)	5
	Fully protected elements (3)	2
IR for availability (A), confidentiality (C) and integrity (I) (5)	Risk realized simultaneously for ACI (1)	10
	Two out of three are affected (AC, AI or CI) (2)	5
	Only one component is at risk (A, C or I) (3)	2

On the basis of the above, the IR risk level of an information-educational environment can be derived as follows:

$$IR = \frac{\sum_{i=1}^n w(IRp_i(t))}{n}$$

The use of weighting factors will make it possible to determine priority areas for reducing the level of IS&IR in the educational environment on the basis on the probabilistic risk modeling.

Discussion of the results

The study of the information aspect of education security has shown a fairly significant number of risks for information systems in education.

At the same time, the range of such risks is constantly expanding due to the specifics of the information processes in education that is consistent with the scientific results of the authors' research [2; 14].

It requires to take into account such risks and to assume system based measures aimed to assess the risks in the context of correlating the definitions "asset", "vulnerability", "threat" and "damage" in the information educational environment.

Accordingly, this scenario-based approach makes it possible to create a general scheme of "security policy" in relation to information risks in education that does not contradict the authors' ideas about such systems [3; 7; 18].

Its implementation is represented as a risk management based on the analysis of the causes and consequences of an IS violation that also allows to analyze the security of the entire information educational environment.

Conclusion

The article attempts to present theoretical argument for the importance of the informatization problem and to identify probable risks for the information educational environment. In addition, there are some requirements for educational content in the modern educational environment to be considered in order to ensure the protection for participants of information interaction.

The adaptive properties of a safe information educational environment are revealed on the basis of an adaptive approach to the construction of educational environment. It will contribute to ensuring secure communication in the information educational space.

The authors have developed and defined a general scheme of "security policy" in relation to information risks in education to provide risk management based on an analysis of the reasons and consequences of IS violations. It can be realized through the authors' assessment method for IS&IR in the educational environment. This method is based on scenarios and allows assessment of existing level of risk, as well as conducting regular security analysis of the entire information educational environment.

The issue of classification of information risks and definition of their criteria remains debatable.

REFERENCES

1. Abramova S.V., Boyarov E.N., Hrapal' L.R., Rubtsova S.Yu. *Informacionnaya bezopasnost' sovremennogo professional'nogo obrazovaniya: problemy, ugrozy, puti resheniya* [Information security of modern professional education: problems, threats, solutions]. *Sovremennye problemy nauki i obrazovaniya*, 2020, no. 6. DOI: 10.17513/spno.30339. (in Russ.)

2. Baranova E. K. *Metodiki analiza i otsenki riskov informatsionnoy bezopasnosti* [Methods of analysis and assessment of information security risks]. *Obrazovatel'nye resursy i tekhnologii*, 2015, no. 1 (9), pp. 73-79. (in Russ.)
3. Belyakova, E.G., Zagvyazinskaya, E.V., Berezentseva, A.I. Student's information culture and informational security. *Education and Science*, 2017, no. 19, p. 8.
4. Bjorn A.G. CORAS, A Platform for Risk Analysis on Security Critical Systems — Model-based Risk Analysis Targeting Security, 2002.
5. Bond M., Buntins K., Bedenlier S. et al. Mapping research in student engagement and educational technology in higher education: a systematic evidence map. *Int J Educ Technol High Educ*, 2020, no.17, DOI: 10.1186/s41239-019-0176-8.
6. Bond, M., Marín, V.I., Dolch, C., Svenja Bedenlier, Olaf Zawacki-Richter. Digital transformation in German higher education: student and teacher perceptions and usage of digital media. *Int J Educ Technol High Educ*, 2018, no. 15. DOI: 10.1186/s41239-018-0130-1.
7. Boyarov E.N. *Klyuchevye problemy informacionnoj bezopasnosti sfery obrazovaniya* [Key problems of information security in the field of education]. *Pedagogika vysshej shkoly*, 2016, vol. 3.1. pp. 42-45.
8. Brown V.J. Risk perception: It's personal. *Environmental Health Perspectives*, 2014, no. 122(10): A276–A279. DOI: 10.1007/s13753-020-00307-5.
9. Bulatov, A.A., Gnatyuk, M.A., Samygin, S.I. *Problemy obespecheniya informacionnoj bezopasnosti molodezhi v prostranstve social'nyx setej* [Problems of ensuring information security of youth in the space of social networks]. *Gumanitarnye, sotsial'no-ekonomicheskie i obshchestvennye nauki*, 2018, no. 8, pp. 16-19. (in Russ.)
10. Burke J.A., Spence P.R., Lachlan K.A. Crisis preparation, media use, and information seeking during Hurricane Ike: Lessons learned for emergency communication. *Journal of Emergency Management*, 2010, no. 8(5), pp. 27–37. DOI: 10.1007/s13753-020-00307-5.
11. Campos N., Nogal M., Caliz C. et al. Simulation-based education including online and on-campus models in different European universities. *Int J Education Technol High Education*, 2020, no. 17, 8. DOI: 10.1186/s41239-020-0181-y.
12. GOST R ISO/IEC 15408-1(2,3)-2002. Methods and means of ensuring security. *Criteria for evaluating the security of information technologies*. Parts 1-3, 2002.
13. Häckel B., Hänsch F., Hertel M., Übelhör J. Assessing IT availability risks in smart factory networks. *Bus Res*, 2019, no. 12. DOI: 10.1007/s40685-018-0071-5.
14. Kiseleva I. A., Iskajyan S.O. *Upravlenie informatsionnymi riskami v biznese* [Information risk management in business]. *Innov: elektronnyy nauchnyy zhurnal*, 2017, no. 1 (30). (in Russ.)
15. Kiseleva I. A., Iskedjian S. O. Information risks: evaluation methods and analysis. *IT-portal*, 2017, no. 2(14). Available at: <http://itportal.ru/science/economy/informatsionnye-riski-metody-otsenk>.
16. Kiseleva I.A., Simonovich N.E. *Problemy bezopasnosti i riska s pozitsii psihologa i ekonomista* [Security issues and the risk from the psychologist and economist positions] Moscow, Novaya realnost Publ., 2016, 148 p.
17. Kolesnikova, I. A. *Higher education in Russia* [Open education: prospects, challenges, and risks]. *Otkrytoe obrazovanie: perspektivy, vyzovy, riski. Vysshee obrazovanie v Rossii*, 2009, no. 7, pp. 12-23.
18. König, L., Jucks, R. When do information seekers trust scientific information? Insights from recipients' evaluations of online video lectures. *Int J Educ Technol High Educ*, 2019, no. 16(1). DOI: 10.1186/s41239-019-0132-7.
19. Kozlov O. A., Romanenko Yu. A. *Riski sovremennogo obrazovaniya v kontekste informatsionnoy bezopasnosti lichnosti* [Risks of modern education in the context of personal information security]. *Innovatsii i investitsii*, 2018, no. 9, pp. 311-314. (in Russ.)
20. Kušar J., Rihar L., Žargi U., Starbek M. Extended risk-analysis model for activities of the project. *SpringerPlus*, 2013, no. 2(227). DOI: 10.1186/2193-1801-2-227
21. Kuzmin V.V. Information risks in post-industrial society. *Manuscript*, 2018, no. 9(95).
22. Mead E., Roser-Renouf C., Rimal R.N., Flora J.A., Maibach E.W., Leiserowitz A. Information seeking about global climate change among adolescents: The role of risk perceptions, efficacy beliefs, and parental influences. *Atlantic Journal of Communication*, 2012, 20(1), pp. 31–52. DOI: 10.1007/s13753-020-00307-5.
23. Mercader C. Gairín J. University teachers' perception of barriers to the use of digital technologies: the importance of the academic discipline. *Int J Educ Technol High Educ*, 2020, no. 17(4). DOI: 10.1186/s41239-020-0182-x.
24. Microsoft Security Assessment Tool. Available at: <https://technet.microsoft.com/ru-ru/security/cc185712.aspx> (accessed 2 March 2021).
25. Palanivel M., Selvadurai K. Risk-driven security testing using risk analysis with threat modeling approach. *SpringerPlus*, 2014, no. 3(754). DOI: 10.1186/2193-1801-3-754.
26. Pask G. Electronic keyboard teaching machines, in *Glaser, R. Lumsdaine, A. (Eds), Teaching Machines and Programmed Learning*, 1960, Vol. 1, Nat. Ed. Assoc., Washington, DC, pp. 336-349.
27. Rehani M.M. Radiation effects and risks: Overview and a new risk perception index. *Radiation Protection Dosimetry*, 2015, no. 165(1-4), pp. 7–9. DOI: 10.1007/s13753-020-00307-5.
28. Sjöberg L. Factors in risk perception. *Risk Analysis*, 2000, 20(1), pp. 1-12. DOI: 10.1007/s13753-020-00307-5.
29. Skinner B. F. *The technology of teaching*, Appleton – Century – Crofts, New York, 1968.
30. Stadtler M., Bromme R. The content–source integration model: A taxonomic description of how readers comprehend conflicting scientific information. In *D. N. Rapp, & J. L. G. Braasch (Eds.), Processing inaccurate*

information: *Theoretical and applied perspectives from cognitive science and the educational sciences*, 2014, (pp. 379–402. Cambridge: The MIT Press. DOI: 10.1186/s41239-019-0132-7.

31. Stankevich P.V., Abramova S.V., Boyarov E.N. Bachelor In Education (Life Safety) Competency Assessment // 18th PCSF 2018 - Professional Culture of the Specialist of the Future. *The European Proceedings of Social & Behavioural Sciences EpSBS*. (December, 30, 2018). vol. 75. pp. 689-700. DOI: 10.15405/epsbs.2018.12.02.75.
32. Yasenev V. N., Dorozhkin A.V., Sochkov A.L. *O kontseptsii provedeniya audita informatsionnoy bezopasnosti v vuze* [On the concept of conducting an information security audit at a university] *Uchet. Analiz. Audit*, 2019, vol. 6, no. 6, pp. 24-33. (in Russ.)
33. Zamula A. A., Odarchenko A. S., Deineko A. A. (2009) Methods of assessment and management of information risks. *Applied Radioelectronics*, 2019, no. 8(3).
34. Zavgorodny V. I. *Informatsionnyy audit i informatsionnye riski* [Information audit and information risks]. *Aktual'nye voprosy ekonomicheskikh nauk*, 2011, no. 19, pp. 377-381. (in Russ.)
35. Zawacki-Richter O., Marín V.I., Bond M., Gouverneur F. Systematic review of research on artificial intelligence applications in higher education – where are the educators? *Int J Educ Technol High Educ*, 2019, no. 16(39). DOI: 10.1186/s41239-019-0171-0.

Информация об авторах

Бояров Евгений Николаевич
(Россия, г. Южно-Сахалинск)

Доцент, доктор педагогических наук, профессор
кафедры безопасности жизнедеятельности
Сахалинский государственный университет
E-mail: e.boyarov@mail.ru
ORCID ID: 0000-0001-7283-1872
SCOPUS ID: 57191878704

Абрамова Светлана Владимировна

(Россия, г. Южно-Сахалинск)

Доцент, доктор педагогических наук, заведующая
кафедрой безопасности жизнедеятельности
Сахалинский государственный университет
E-mail: abramova_sv@list.ru
ORCID ID: 0000-0002-9863-5287
SCOPUS ID: 57191872091

Станкевич Петр Владимирович

(Россия, г. Санкт-Петербург)

Профессор, доктор педагогических наук,
Декан факультета безопасности жизнедеятельности
Российский государственный педагогический
университет им. А.И.Герцена
E-mail: p_v_stan@mail.ru
ORCID ID: 0000-0001-6506-7968
SCOPUS ID: 57191877822

Корнеева Инна Владимировна

(Россия, г. Южно-Сахалинск)

Доцент, кандидат филологических наук,
Заведующая кафедрой иностранного языка и
страноведения
Сахалинский государственный университет
E-mail: verkor@mail.ru
ORCID ID: 0000-0002-4647-1970

Information about the authors

Evgeniy N. Boyarov

(Russia, Yuzhno-Sakhalinsk)

Doctor of Pedagogical, Associate Professor,
Professor of Department of Life Safety
Sakhalin State University
E-mail: e.boyarov@mail.ru
ORCID ID: 0000-0001-7283-1872
SCOPUS ID: 57191878704

Svetlana V. Abramova

(Russia, Yuzhno-Sakhalinsk)

Doctor of Pedagogical, associate Professor,
Head of Department of Life Safety
Sakhalin State University
E-mail: abramova_sv@list.ru
ORCID ID: 0000-0002-9863-5287
SCOPUS ID: 57191872091

Petr V. Stankevich

(Russia, Saint-Petersburg)

Doctor of Pedagogical Sciences,
Professor,
Dean of the Faculty of Life Safety
Herzen State Pedagogical University of Russia
E-mail: p_v_stan@mail.ru
ORCID ID: 0000-0001-6506-7968
SCOPUS ID: 57191877822

Inna V. Korneeva

(Russia, Yuzhno-Sakhalinsk)

PhD in Philological Sciences, Associate Professor,
Head of Department of Foreign Language and Regional
Studies
Sakhalin State University
E-mail: verkor@mail.ru
ORCID ID: 0000-0002-4647-1970