SDG
JOURNAL OF LAW AND SUSTAINABLE DEVELOPMENT
ISSN: 2764-4170

DEVELOPMENT OF COMPETENCE IN THE SPHERE OF INFORMATION SECURITY TO ACHIEVE SUSTAINABLE DEVELOPMENT

[1]Vladimir Biryukov, [2]Elena Nemtchinova, [3]Tatyana Pavlova, [4]Ashot Kagosyan & [5]Tatyana Avdeeva

ABSTRACT

Objective: Global information and technological changes have opened up new opportunities for information and public communication processes. The purpose of the study is to analyze the level of competence of future specialists in economics and finances in the field of information security and develop recommendations for its improvement.

Methods: The level of information security competencies of future specialists in economics and finance has been determined, characterized by the degree of awareness of the importance of readiness to work in corporate information security systems based on an empirical study using a survey of "Finance, banking, and insurance", "Accounting and taxation", and "Economics" students (94 people total) and a subsequent pedagogical experiment with their participation.

Results: Authors of the articles have described the main methods and directions of forming the ability of a future specialist in economics and finance to work responsibly in corporate institutions, which are associated, first of all, with the introduction of a special course "Security of financial and economic information in information systems".

Conclusion: The lack of readiness among economics and finance specialists to work in corporate information security systems may hinder the achievement of sustainable development. To address this issue, it is important to prepare future specialists in economics and finance for professional activity in the conditions of a corporate information security system. It is possible to prevent the development of negative phenomena in the field of information security with the help of the purposeful formation of appropriate competencies in specialists in economics and finance.

Keywords: Corporate information. Information security. Information security system. Sustainable development

Received: 15/10/2022
Accepted: 23/01/2023
DOI: https://doi.org/10.37497/sdgs.v11i1.267

[1] Moscow Polytechnic University, (Russia). E-mail: vladimir.a.biryukov@gmail.com Orcid id: https://orcid.org/0000-0002-2580-5927
[2] Russian State University of Tourism and Service, (Russia). E-mail: e.e.nemtchinova@mail.ru Orcid id: https://orcid.org/0000-0001-5293-468X
[3] Moscow Aviation Institute, (Russia). E-mail: vptp52@mail.ru Orcid id: https://orcid.org/0000-0002-2674-496X
[4] Gzhel State University, (Russia). E-mail: Aksochi@rambler.ru Orcid id: https://orcid.org/0000-0002-9785-5835
[5] State University of Humanities and Technology, (Russia). E-mail: avdeeva-t-i@mail.ru Orcid id: https://orcid.org/0000-0002-9419-2191

Biryukov, V., Nemtchinova, E., Pavlova, T., Kagosyan, A., & Avdeeva, T. (2023). Development of competence in the sphere of information security to achieve sustainable development. *Journal of Law and Sustainable Development*, *11*(1), e0267. https://doi.org/10.37497/sdgs.v11i1.267

DESENVOLVIMENTO DE COMPETÊNCIA NO ÂMBITO DA SEGURANÇA DA INFORMAÇÃO PARA ALCANÇAR O DESENVOLVIMENTO SUSTENTÁVEL

RESUMO

Objetivo: A informação global e as mudanças tecnológicas abriram novas oportunidades para os processos de informação e comunicação pública. O objetivo do estudo é analisar o nível de competência dos futuros especialistas em economia e finanças na área de segurança da informação e desenvolver recomendações para sua melhoria.

Métodos: Foi determinado o nível de competências em segurança da informação dos futuros especialistas em economia e finanças, caracterizado pelo grau de consciência da importância da prontidão para trabalhar em sistemas de segurança da informação corporativa com base em um estudo empírico usando uma pesquisa de "Finanças, bancos , e seguros", alunos de "Contabilidade e Fiscalidade" e "Economia" (94 pessoas no total) e uma posterior experiência pedagógica com a sua participação.

Resultados: Os autores dos artigos descreveram os principais métodos e orientações para formar a capacidade de um futuro especialista em economia e finanças para trabalhar com responsabilidade em instituições corporativas, associadas, antes de tudo, à introdução de um curso especial "Segurança de informações financeiras e econômicas em sistemas de informação".

Conclusão: A falta de preparo dos especialistas em economia e finanças para atuar em sistemas de segurança da informação corporativa pode dificultar o alcance do desenvolvimento sustentável. Para enfrentar esta questão, é importante preparar os futuros especialistas em economia e finanças para a atividade profissional nas condições de um sistema corporativo de segurança da informação. É possível prevenir o desenvolvimento de fenômenos negativos no campo da segurança da informação com a ajuda da formação proposital de competências apropriadas em especialistas em economia e finanças.

Palavras-chave: Informação corporativa. Segurança da informação. Sistema de segurança da informação. Desenvolvimento sustentável

Biryukov, V., Nemtchinova, E., Pavlova, T., Kagosyan, A., & Avdeeva, T. (2023). Development of competence in the sphere of information security to achieve sustainable development. *Journal of Law and Sustainable Development*, *11*(1), e0267. https://doi.org/10.37497/sdgs.v11i1.267

DESARROLLO DE COMPETENCIAS EN EL ÁMBITO DE LA SEGURIDAD DE LA INFORMACIÓN PARA ALCANZAR EL DESARROLLO SOSTENIBLE

RESUMEN

Objetivo: La información global y los cambios tecnológicos han abierto nuevas oportunidades para los procesos de información y comunicación pública. El propósito del estudio es analizar el nivel de competencia de los futuros especialistas en economía y finanzas en el campo de la seguridad de la información y desarrollar recomendaciones para su mejora.

Métodos: Se ha determinado el nivel de competencias en seguridad de la información de los futuros especialistas en economía y finanzas, caracterizado por el grado de conciencia de la importancia de la preparación para trabajar en los sistemas de seguridad de la información corporativa a partir de un estudio empírico mediante una encuesta de “Finanzas, banca y seguros”, “Contabilidad y tributación” y estudiantes de “Economía” (94 personas en total) y una posterior experiencia pedagógica con su participación.

Resultados: Los autores de los artículos han descrito los principales métodos y direcciones para formar la capacidad de un futuro especialista en economía y finanzas para trabajar de manera responsable en instituciones corporativas, que están asociadas, en primer lugar, con la introducción de un curso especial "Seguridad de información financiera y económica en los sistemas de información".

Conclusión: La falta de preparación de los especialistas en economía y finanzas para trabajar en sistemas de seguridad de la información corporativa puede dificultar el logro del desarrollo sostenible. Para abordar este tema, es importante preparar a los futuros especialistas en economía y finanzas para la actividad profesional en las condiciones de un sistema de seguridad de la información empresarial. Es posible prevenir el desarrollo de fenómenos negativos en el campo de la seguridad de la información con la ayuda de la formación deliberada de competencias apropiadas en especialistas en economía y finanzas.

Palabras clave: Información corporativa. Seguridad de la información. Sistema de seguridad de la información. Desarrollo sostenible

INTRODUCTION

The relevance of compliance with information security requirements by subjects of economic relations has increased in the context of the globalization of economic processes, the expansion of ties between countries, the search for new markets for products, and the struggle for them, as well as based on the difficult economic situation (Lochan et al., 2021; Ramazanov et al., 2023). Regardless of the form of ownership and the profile of activity, each institution strives to securely store corporate information, especially financial information, which is increasingly becoming the object of illegal actions, investing in technical equipment and

appropriate qualifications of employees for this purpose (Grundel et al., 2020; Huy Binh, Kien, 2021). Protecting and preserving information in corporate systems, which are significant resources of organizations, are extremely important problems for organizations and their specialists (Khoruzhy et al., 2022).

According to the degree of criminal activity, credit, accounting, currency, and stock transactions require the greatest attention concerning protection (Tsokur et al., 2020). Recently, the list of such operations has been expanding, and they are acquiring new features in connection with the dynamic spread of information, computing, and payment systems, technologies for the remote provision of financial services, electronic exchange, e-commerce, and the Internet of Things (Avdeev et al., 2022). This, in turn, forms new requirements for information security systems (Iskajyan et al., 2022).

In connection with the above, insufficient adaptability to the actual conditions of performance of professional duties in corporate systems (Chupanova et al., 2021) engaged in financial and economic activities and readiness to preserve and protect confidential corporate information should be noted among the main contradictions of modern professional training of future specialists in economics and finance (Manuylenko et al., 2022).

The development of information security systems is happening so fast that this circumstance underlines the relevance of the chosen problem and encourages universities and companies themselves to carefully approach the training of future specialists in economics and finance in the formation of information security competencies.

LITERATURE REVIEW

The problem of information protection is of interest to scholars of various branches of science: programming, computer networks, and information protection (Sedova et al., 2023; Neverov et al., 2022), law (Pauzin et al., 2022), information security management (Gavrilov et al., 2022). Thus, we note that this problem is mainly dealt with by specialists in the field of physical and mathematical (Tolmachev et al., 2022) and technical (Logachev et al., 2022) sciences, whose research is intended for official use, since it contains technical developments of information security systems.

The analysis of the scientific heritage in the field of pedagogical sciences revealed that the problem of training specialists in the field of information security is reflected in studies on problem-based information security training (Popov et al., 2021), the development of a multimedia course on information security, and the use of information technologies for training

information security specialists (Skripak et al., 2022). Along with this, the problem of the formation of information security competencies in the process of training specialists in economics and finance has not been considered.

The importance of this issue is determined by the fact that any specialist of a financial and economic profile, exercising their professional duties, is forced to work in a corporate information protection system and comply with instructions on the safety of corporate information.

The study (Bobrova et al., 2021) shows that a specialist can: 1) treat corporate information unconsciously and disclose its contents; 2) be irresponsible by losing operational information, as well as keys and access codes, or not ensuring its safety; 3) show a lack of determination concerning illusory prospects of enrichment, through fraudulent actions or theft of funds.

Thus, according to (Chapman, 2021), the following information is of the greatest interest in the economic environment:

- commercial information: summary reports on the financial activities of the company (monthly, quarterly, annual, for several years); loan agreements with banks; purchase and sale agreements; information about promising sales markets, sources of raw materials and goods, or profitable partners; information provided by partners if penalties are provided for its disclosure; information about the place of storage of goods and time and routes of their transportation; identification of persons promising for recruitment by bribery, blackmail, or another method; communications and management capabilities (Niemimaa, Niemimaa, 2017);

- personal information: the sources of income of the management; the order of the personal life of the head and their family members; the schedule and addresses of business and personal meetings (Niemimaa, Niemimaa, 2017); information about human weaknesses; addictions; bad habits; sexual orientation; data on leisure activities, routes of movement; information about places of storage of valuables; residence location.

Consequently, the problem of economics and finance specialists' readiness to meet the requirements of information security in corporate information systems is still unresolved and relevant.

The purpose of the study is to analyze the level of competence of future specialists in economics and finance in the field of information security and develop recommendations for its improvement.

Research objectives:

1. surveying to identify the awareness of future specialists in economics and finance of the importance of forming readiness to work in corporate information security systems;

2. development and testing of a set of life situations related to the possibility of disclosure of commercial or personal information that could harm the organization;

3. obtaining results on the level of information security competence of future specialists in economics and finance.

METHODS

An approximate set of theoretical and empirical research methods was determined to achieve the research goal:

theoretical methods (analysis, synthesis, comparison, generalization) – for the study of scientific literature on the problem of the formation of competencies of future specialists in the field of information security;

empirical methods (survey method, method of pedagogical experiment) – to determine the level of information security competence in future specialists in economics and finance.

The experimental study included the following stages:

- surveying to identify the awareness of future specialists in economics and finance of the importance of forming readiness to work in corporate information security systems;

- development and analysis of a set of life situations related to the possibility of disclosure of commercial or personal information that could harm the organization;

- analysis of the study results.

The criterion of the level of information security competence of future specialists in economics and finance was,

firstly, their awareness of the importance of forming readiness to work in corporate information security systems (to describe it, a questionnaire was developed that provides a free form of response);

secondly, the availability of practical skills to preserve various types of confidential information (to describe it, a set of life situations related to the possibility of disclosure of commercial or personal information that could harm the organization was specially developed). Their analysis made it possible to form the readiness of future specialists in the financial and economic field to preserve various types of confidential information. Strengthening the professional orientation of the training of future financiers has made it possible to achieve the necessary level of awareness of future financiers with responsibilities to preserve confidential information.

The study involved "Finance, Banking, and Insurance", "Accounting and taxation", and "Economics" students (a total of 94 people).

The percentage of correctly resolved situations by students related to the preservation of confidential commercial and personal information was determined using the G-sign test during the mathematical processing of the research results.

Null and alternative hypotheses were formulated.

H0: The increase in the number of situations correctly resolved by students is accidental.

H1: The increase in the number of situations correctly resolved by students is not accidental.

Critical values of the G-sign test: 38 ($p < 0.05$); 35 ($p < 0.01$).

The calculation of the G-sign test was carried out by compiling a corresponding table using Microsoft Excel.

RESULTS

First of all, we consider it necessary to explain the specifics of the problems that representatives of the financial sector of the economy face in Russia when discussing security issues. Let us give an example of a situation where information is leaked from banks for a better understanding of the respondents' response. In 2021, 20 ads for the sale of new databases of banking clients in Russia were registered on DarkNet. Thus, three of the 20 databases contained more than 100 thousand customer records: information about 150 thousand people willing to take loans from Sovcombank and about 100 thousand from DOM.RF Bank, as well as an offer to sell the data of half a million Sberbank Premier customers (Sberbank's special program for servicing regular customers on privileged conditions). This data is usually used by attackers who call people from leaked databases on behalf of the bank security service or law enforcement agencies to steal money from a bank account (Tadviser, 2021).

A survey of students on the importance and significance of building readiness to work in corporate information security systems showed that they do not fully understand the significance of the existing problem described in the example of bank card data leakage. In particular, 72.8% of respondents claim that the protection of information is not their task as a future financier, but the task of a certain department of the organization, that is, specialist engineers servicing the protection system; they do not see their involvement in the preservation of corporate information.

28.3 % of respondents answered in affirmatively to the question "Can you freely use the closed information of an institution among your friends?", which indicates that they are unaware of the essence of closed corporate information.

82.9 % of respondents, answered the question "As is known, the leaders of an organization have the highest level of access to classified information, and employees, depending on their rank and position, have a lower level of access to it. Who, in your opinion, causes more harm to the interests of the organization?", and believe that managers, having the opportunity to use classified information, cause the greatest harm. However, this is not confirmed by the results of the studies (Avdeev et al., 2022), since such cases are exceptional and isolated, and it is middle managers and employees who cause the greatest harm.

The results of experimental work aimed at students' ability to resolve life situations related to the possibility of disclosure of commercial or personal information that could harm the organization are presented in Table 1.

Table 1. Results of the pedagogical experiment

Situations	**Proper solution to the situation, %**	
	Before the experiment	**At the end of the experiment**
preservation of confidential commercial information	31.7 %	23.7 %
preservation of confidential personal information	72.4 %	49.3 %

Thus, if only 31.7 % of students were able to correctly solve situations related to the preservation of confidential commercial information at the beginning of the experimental work, and 23.7 % – with the preservation of confidential personal information, then at the end of the experiment 72.4 % of students correctly solved situations of the first type and 49.3 % were able to solve situations of the second type.

The statistical probability of an increase in the number of situations correctly resolved by students at two levels of significance is confirmed by the calculation of the G-sign test (Gemp = 8; Gemp. < Gcr).

DISCUSSION

The results of our survey showed that future specialists do not realize the importance and necessity of information protection in their daily professional activities, have a low level of readiness to work in corporate information protection systems.

The study (Niemimaa, Niemimaa, 2017) revealed that the majority of violations (81.7 %) are carried out by employees of the organization who have access to its system, and only 17.3 % of violations are committed by outsiders. Using the results of this study, we emphasize that the clarification of the motives of the requirements violations of the information protection system by employees of organizations revealed that 10 % of them were committed by offended and dissatisfied employees-users of the corporate information protection system, about 10 % – by staff for selfish reasons, but most (50-55 %) are the result of unintentional errors, the consequence of negligence, irresponsibility or incompetence of the personnel and/or users of the system. This figure is significant enough to be taken into account, which, in turn, raised the question of identifying the nature of these violations and the reasons for the incompetence of employees as users of the corporate information protection system.

In addition, the problems of information leakage became even more acute during the remote work of employees due to insufficient compliance with information security standards outside the workplace and the lack of external control over compliance with information security.

In our opinion, the reason for the weak awareness of the importance and necessity of information protection in everyday professional activities is, among other things, in the plans and programs of professionally-oriented training of specialists. Today, the processes of reforming and institutional transformation of higher education are deepening, where the quality of education is determined by one of the main priorities, the prerequisites of which, along with material and technical support and human resources, create meaningful professionally-oriented and innovative educational programs (Korneev et al., 2022).

Thus, classical and economics universities account for only 29.35% of the market of educational services for training specialists in economics and finance, and its large share falls on non-core universities, where specialists are trained mainly in the "Finance, banking, and insurance" and "Accounting and taxation" specialties (Skripak et al., 2022). Along with this, we observe a lack of formulation and inclusion in general and/or special information security competencies.

The analysis of a specially developed set of life situations related to the possibility of disclosure of commercial or personal information that could harm the organization allowed forming the readiness of future specialists in the financial and economic field to preserve various types of confidential information. Strengthening the professional orientation of the training of future financiers has made it possible to achieve the necessary level of awareness of future financiers with responsibilities to preserve confidential information.

In our opinion, the essence of information security competence lies in the professional characteristics of economics and finance specialists, and its content is formed by the following: knowledge about the place and role of information security, legal foundations, principles, and methods of organizing the protection of corporate information, as well as countering manifestations of unauthorized information exposure and information leakage, taking into account the behavioral aspects of personnel; the ability to formulate and implement policies, analyze and assess threats and implement measures to counter information security violations in a specific professional field; skills in analyzing and formalizing information processes, forming requirements for information security systems.

The acquisition of information security competence of economics and finance specialists can be solved by including new academic disciplines in educational programs or a block of general training disciplines, or selective special disciplines, for example, by introducing the "Security of financial and economic information in information systems" course. Also, it is advisable to include certain topics on ensuring the security of financial and economic information in the thematic plan of professional disciplines of specialties.

The following is highlighted in the system of protection of confidential information (be it banking or commercial corporate secrets): the legislative and legal component, which is presented in the legislation; the regulatory component, which is determined by the management of the organization; the organizational structure (special units or employees who ensure the implementation of the security policy) and the security policy (Niemimaa, Niemimaa, 2017). Some scholars (Avdeev et al., 2022) include users in the security system, arguing that they have a direct influence on it, others (Khoruzhy et al., 2022) do not share this opinion. The regulatory component of the organization's security system should include the following: a collective agreement, labor contracts; instructions on how to work with information constituting a trade secret; order on the admission of employees to information constituting a trade secret, the employee's obligations to adhere to the established information protection regime (Chapman et al., 2021).

We believe that a future specialist (bank employee, insurance company employee, firm financier, accountant, auditor, etc.) should go through the initial stage of adaptation to the conditions of professional activity in the process of professional training already at universities. They should understand the essence of the requirements that the information security system imposes on employees, in which there is confidential commercial information subject to storage and protection. The requirements of the banking system to its employees are the most complete, which is why, in our opinion, it is better to acquaint students with their content.

The results of the study indicate that starting to perform professional duties, a young specialist should understand that the problem of protecting and storing information, which is a significant resource in organizations engaged in financial, insurance, or industrial activities, is very important. Since employees of the company are involved in the use of this information at different levels of access, there is also a problem of forming the readiness of personnel to preserve corporate information and protect it. Scholars (Crossler et al.,2013) consider potentially dangerous those persons who are not able to fulfill the requirements of the internal security regime of the company.

It was revealed in the course of the study that it is necessary to characterize the specifics of the activities of various enterprises, organizations, institutions, and firms in more detail within which the professional activity of the future specialist will take place. This concerns the content of confidential information and trade secrets, protection systems because they differ too much in their parameters and tasks, information access systems, and working conditions.

CONCLUSION

An insufficient level of readiness of economics and finance specialists to work in corporate information security systems has been revealed despite the urgency of the problem of preparing an economics and finance specialist for professional activity in corporate information security systems.

We consider it important to prepare future specialists in economics and finance for professional activity in the conditions of a corporate information security system to prevent violations in the field of information security related to negligence and even cybercrime. The article defines the main methods and directions of forming the ability of a future financier to work responsibly in corporate institutions, which we associate primarily with the introduction of a special "Security of financial and economic information in information systems" course. The perspective of the study may be the analysis of the specifics of the subject area of the specified special course and its testing on a larger sample of students.

REFERENCES

Avdeev, V., Avdeeva, O., Bulygina, J., Byzova, I., Aksenov, A. (2022). Modernization of legal technologies in the field of personal and information security. Revista Relações Internacionais do Mundo Atual, 1(34). http://dx.doi.org/10.21902/Revrima.v1i34.5981

Bobrova, S. E., Popova, E. N., Sizova, Y. S., Orlova, L. N., & Polozhentseva, I. V. (2021). Professional foreign language competence formation using educational multimedia technologies. International Journal of Education and Practice, 9(1), 155–170. https://doi.org/10.18488/journal.61.2021.91.155.170

Chapman, P. (2021). Defending against insider threats with network security's eighth layer. Computer Fraud and Security, 2021(3), 8–13. https://doi.org/10.1016/S1361-3723(21)00029-4

Chupanova, K. A., Otrokov, O. Y., Mosina, N. V., Sekerin, V. D., Zharov, A. N., & Garnik, S. V. (2021). Supply Chain Management Concept and Digital Economy: Digital Supply Chain Technological Innovation. Indian Journal of Economics and Development, 17(4), 928–933. https://doi.org/10.35716/IJED/21272

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers and Security, 32, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Gavrilov, B. Y., Voronin, M. Y., Sizova, V. N., Lapin, V. O., Demidova-Petrova, E. V. (2022). Trends of the criminal-legal complex in relation to the legislative consolidation of the misdemeanor catego. JURÍDICAS CUC, 18(1), 183–198. https://doi.org/10.17981/juridcuc.18.1.2022.08

Grundel, L. P., Malis, N. I., Zhuravleva, I. A., Melnikova, N. P., & Mandroshchenko, O. V. (2020). Promising information technologies for tax purposes: International trends in software for auditors. International Journal of Engineering Research and Technology, 13(11), 3977–3986. https://doi.org/10.37624/ijert/13.11.2020.3977-3986

Huy Binh, N., Kien, L.T. (2021). Counteraction against digital data leak: Open source software for intrusion detection and prevention. International Journal of Engineering Trends and Technology, 69(3), 17–22. https://doi.org/10.14445/22315381/IJETT-V69I3P204

Iskajyan, S. O., Kiseleva, I. A., Tramova, A. M., Timofeev, A. G., Mambetova, F. A., & Mustaev, M. M. (2022). Importance of the Information Environment Factor in Assessing a Country's Economic Security in the Digital Economy. International Journal of Safety and Security Engineering, 12(6), 691–697. https://doi.org/10.18280/ijsse.120604

Khoruzhy, L. I., Katkov, Y. N., Romanova, A. A., Katkova, E. A., & Dzhikiya, M. K. (2022). Adaptive management reporting system in inter-organizational relations of agricultural enterprises according to ESG principles. Journal of Infrastructure, Policy and Development, 6(2). https://doi.org/10.24294/jipd.v6i2.1649

Korneev, D.G., Gasparian, M.S., Gavrilov, A.V., Sysoev, N.A., Filyuk, M.A. (2022). Creating a service-oriented information and educational space. International Journal of Emerging Technology and Advanced Engineering, 12(2), 153–158. https://doi.org/10.46338/ijetae022_18

Lochan, S. A., Rozanova, T. P., Bezpalov, V. V., & Fedyunin, D. V. (2021). Supply chain management and risk management in an environment of stochastic uncertainty (Retail). Risks, 9(11). https://doi.org/10.3390/risks9110197

Logachev, M. S., Laamarti, Y. A., Rudneva, S. E., Ekimov, A. I., Zemlyakov, D. N., Barkov, A. (2022). Information System for Monitoring and Management of the Quality of Educational Programs: Development of Functioning Algorithms. International Journal of Instruction, 15(3), 429–450. https://doi.org/10.29333/iji.2022.15324a

Manuylenko, V. V., Ermakova, G. A., Gryzunova, N. V., Koniagina, M. N., Milenkov, A. V., Setchenkova, L. A., & Ochkolda, I. I. (2022). Generation and Assessment of Intellectual and Informational Capital as a Foundation for Corporations' Digital Innovations in the "Open Innovation" System. International Journal of Advanced Computer Science and Applications, 13(9), 922–932. https://doi.org/10.14569/IJACSA.2022.01309118

Neverov, E. N., Korotkiy, I. A., Korotkih, P. S., Mokrushin, M. Y. (2022). Improving the Environmental Efficiency of Engineering Systems Operating under the Scheme of Secondary Use of Thermal Energy. International Journal of Heat and Technology, 40(6), 1533–1539. https://doi.org/10.18280/ijht.400623

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. European Journal of Information Systems, 26(1), 1–20. https://doi.org/10.1057/s41303-016-0025-y

Pauzin, N., Vasyukov, V., Krasheninnikov, S., Yudina, E. (2022). Law Enforcement and Social Security of Public Events: Organizational and Legal Solutions. Journal of Law and Sustainable Development, 10(1), e0239. https://doi.org/10.37497/sdgs.v10i1.239

Popov, V.N., Vasilenko, V.N., Khvostov, V.A., Denisenko, V.V., Skrypnikov, A.V., Ivanov, A.V., Belyaev, A.N., Stukalo, O.G. (2021). Security threats to personal data in the implementation of distance educational services using mobile technologies. Journal of Theoretical and Applied Information Technology, 99, 3935–3946.

Ramazanov, I., Panasenko, S., Stolyarova, A., Mayorova, E., Nikishin, A., & Pankina, T. (2023). Innovative potential and problems of sustainable development of the sphere of circulation in the russian federation. Journal of Law and Sustainable Development, 11(1), e0266. https://doi.org/10.37497/sdgs.v11i1.266

Sedova, O. V., Alekseev, A. G. (2023). Development of Mathematical Models To Determine The Balance Of The System Of Platform Interactions When Scaling The End-To-End Monitoring Process For Priority Sectors Of The Economy. Journal of Theoretical and Applied Information Technology, 101(1), 11–20.

Skripak, I. A., Shatskaya, A. V., Ukhanova, E. V., Tkachenko, A. E., & Simonova, N. A. (2022). Information Technologies and Language: The Impact of CAT Systems on Improving the Efficiency of Translators' Training. Theory and Practice in Language Studies, 12(11), 2358–2364. https://doi.org/10.17507/tpls.1211.16

Tadviser. (2021). Utechki dannykh iz bankov Rossii [Data leaks from Russian banks]. Retrieved from: https://www.tadviser.ru/index.php/Статья:Утечки_данных_из_банков_России

Tolmachev, M., Korotaeva, I., Zharov, A., Beloglazova, L. (2022). Development of Students' Digital Competence When Using the "Oracle" Electronic Portal. European Journal of Contemporary Education, 11(4), 1261–1270. https://doi.org/10.13187/ejced.2022.4.1261

Tsokur, E., Kharitonova, O., Evreeva, O., Lobazova, O., Magomedov, R., Panikarova, N.F. (2020). Information technology for decision-making on territory management and interaction with the population. COMPUSOFT: An International Journal of Advanced Computer Technology, 9(10), 3886–3891.