Innovative information security methods for vertically integrated companies

Nikita Loginov[1], *Maria* Sysoenko[1*], and *Elena* Pavlova[1]

[1] ITMO University, St. Petersburg, Russia

Abstract. The article is devoted to the study of methods for ensuring information security for vertically integrated companies. The study examined the concept of a vertically integrated company, studied its features, risks, information security structure and key components of its software. The authors analyzed modern methods and tools for ensuring cybersecurity, applicable in the analyzed companies, and carried out a comparative analysis of their advantages and disadvantages. The work mentions integrated information security systems. Particular attention is paid to authentication technology based on SIM cards with an electronic digital signature as one of its mechanisms. The article examines tokens as traditional tools for implementing electronic digital signatures and SIM cards from the point of view of more modern technology, and also carries out a comparative analysis of them from the economic, technical and legal aspects. The work describes and visualizes a diagram of the process of installing tokens and SIM cards in the business process of vertically integrated companies, and the process of replacing tokens with SIM cards is considered from three points of view: economic, technical and legal. The result of the study was the expansion of the existing knowledge base about ensuring information security in vertically integrated companies and the identification of the implementation of SIM card-based authentication technology as prevailing in relation to the token-based authentication system.

1 Introduction

The chosen research topic is of high relevance in the modern information society, where ensuring reliable data protection is becoming an increasingly priority area of development. Cyber-attacks, leaks of confidential information, malware and other types of security breaches threaten both the personal data of users and the existence and development of companies - especially for vertically integrated companies (hereinafter referred to as VIC). VIC controls and manages all stages of production and service provision in the field of activity, combining several levels of vertical integration, including production, distribution, sales and maintenance of equipment and services. These companies have access to vast amounts of information, including customer personal data, transaction data and trade secrets, and much of their business processes and communications are conducted over the Internet

* Corresponding author: sysoenko.m@yandex.ru

and communications networks, making them especially vulnerable to new and evolving types of cyber threats.

The need to develop effective methods and means of ensuring information security for VIC becomes especially relevant in light of the rapid development of technology. Today, the cybersecurity market offers various modern encryption algorithms, multi-factor authentication systems, firewalls and intrusion detection systems. However, the use of only these individual solutions does not always guarantee complete protection of information systems. With the increase in cybersecurity criminal activity, the development of new attack methods and the introduction of new 5G and IoT technologies, large VICs are increasingly recognizing the need to apply strong techniques and develop their own approaches to information security.

At the end of 2021, the total number of open sources of leakage of confidential information from companies and authorities in the Russian Federation was 1,729 cases, which is 28.1% less than in 2020, although the country still ranks second after the United States in the number of incidents. Of these, more than 60% of cases occurred as a result of the actions of external attackers, which is noticeably different from previous years, when the main source of information security violations were company employees. Today, the share of personal data leaks that occurred without the use of automation tools has decreased from 14.1% to 4.5% over four years, which indicates an increase in the digitalization of the country. The Internet remains the main channel for data leaks - compromise of data from networked corporate systems and cloud storage, and high-tech companies, healthcare organizations and the public sector are leaders in this issue.

However, it should be noted that over the past 5 years, the legislation of the Russian Federation in the field of data protection and privacy has undergone a number of changes. In 2019, amendments were made to the Federal Law «On Personal Data», and in 2020 a package of laws on the processing of personal data (LOPD) and a new Federal Law «On amendments to certain legislative acts of the Russian Federation on the processing of personal data in information systems» that emphasize the importance of protecting personal data from illegal access, modification and distribution, as well as introducing mandatory user authentication to access such data and implementing measures to prevent information leaks.

2 Formulation of the problem

The purpose of the study is to identify effective methods of ensuring information security for vertically integrated companies.

To achieve this goal, it is necessary to complete the following tasks:

– study the features and risks of VIC when ensuring information security;

– analyze modern methods and tools for ensuring information security applicable in VIC;

– compare the advantages and disadvantages of using various information security methods in the VIC from the economic, technical and legal aspects;

– formulate practical recommendations for improving the VIC information security system using modern technologies.

3 Literature review

Topoleva T.N., Zhukovskaya I.E., Matveev A.V., Shatsky M.S., Okumbekova M., Subbotin A.S., Biryukova V.V. dealt with the issue of describing vertically integrated systems. [3, 9, 13, 14, 18, 19]. Topoleva T.N. identified the organizational structure of the VIC in the context of information security and presented a model of key functional units [18]. Zhukovskaya E.I. studied modern trends in the field of information security - the use of artificial intelligence

and machine learning to detect attacks and protect data [19]. Matveev A.V. and Shatsky M.S. considered the importance of creating a safety culture at all levels of the company and implementing appropriate policies and procedures [9]. Okumbekova M. examined data protection methods and emphasized the importance of using modern technologies to ensure data security in vertically integrated companies [13]. In the work of Subbotin A.S., strategies are proposed for effective vulnerability management and timely response [14]. In the dissertation of Biryukova V.V., methods for ensuring compliance with regulatory requirements and standards in vertically integrated companies are explored, and the results obtained allow us to identify best practices in the field of compliance and develop a strategy for complying with existing regulations [3].

A number of foreign authors have dealt with the issue of information and cyber security. Nosova E.A., Anisimova L.V., Murovana T.S., Svyatiuk Yu.A. and Yafinovich E.R. presented an overview and analysis of key aspects and principles of the economics of information security [12]. Alok M., Alzoubi Y.I., Anwar M.J. and Gill A.K. analyzed the main attributes and factors that matter in the formation and application of cybersecurity policies in the USA, EU, Canada, Australia, China, India and Malaysia [10]. Kremer F.'s work examines cyber risk and cybersecurity from the point of view of the availability and openness of information about this phenomenon [8].

Methods for improving business processes in a company, the mechanisms of operation of eSIM and digital signature technology, and methods for their implementation in the field of the Internet of Things attract researchers around the world. Tan G.T., Pawel Salachowski and Jianin Ch. reviewed alternative digital signature methods based on post-quantum algorithms and determined their impact on the security of existing cryptographic systems [17]. Al Musa A., Al-Komri M., Al Hajri S. and Zagruba R. presented the concept of using eSIM to generate, store public key encryption keys and manage the authentication and signing process of digital messages [1]. Antokhin Yu.N. studied the use of electronic SIM cards and digital signatures to improve business processes in companies [2]. Sukhmitsingh G. described the advantages of using SIM cards compared to tokens, and Surabhi T. reviewed their technical aspects [15, 16].

It should be noted that a search for modern literature sources on the problem under study shows their insufficiency. In current research, the authors conclude that VICs face unique challenges and threats to information security, and understanding these aspects and developing appropriate security methods and approaches are necessary for the effective operation and protection of data in such companies.

4 Research methodology

The study used methods for analyzing modern information security tools applicable in the VIC, and carried out a comparative analysis of their advantages and disadvantages from the point of view of economic and technical legal aspects. To assess risks in the implementation of information security at VIC, a risk assessment map was built and analyzed in order to identify the most likely and most powerful threats. As part of the study, the legislative and legal norms governing information security in the Russian Federation were studied. Based on the analysis, practical recommendations were formulated to improve the VIC information security system using SIM card technology with digital signature. For clarity of the proposed solutions, visualization was carried out using diagrams.

5 Results

VICs have certain features that are important to consider when implementing information security methods. The network infrastructure of companies combines various functional areas, in which each level has its own vulnerabilities and threats, which creates difficulties in ensuring high-quality security of the entire network perimeter, and active interaction with other organizations, contractors and suppliers creates a condition for ensuring security at all levels of interaction. As noted earlier, VICs work with a large volume of confidential information, which is why they are subject to regulatory requirements of laws on the protection of personal data, which creates the need to establish appropriate security procedures.

There is a certain set of options for authentication tools on the Russian market. The choice of a specific one is based on the needs of the organization, depending on ease of use and level of protection. The list of authentication means is presented in Figure 1.

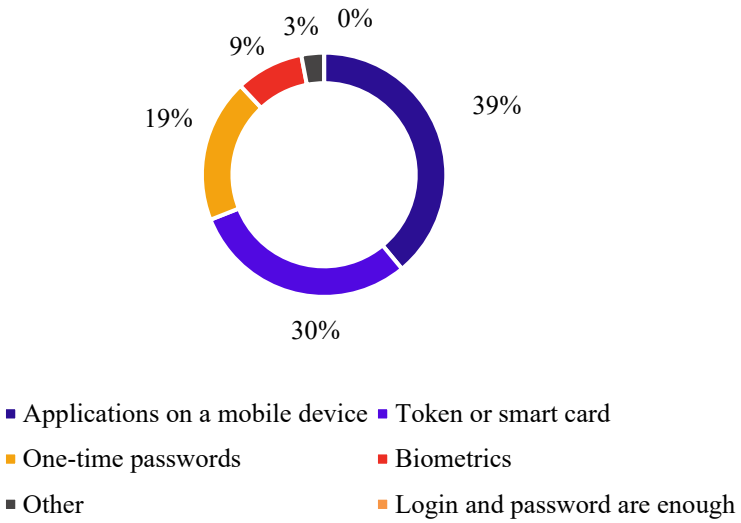

Fig. 1. Authentication technology market. Source: developed by the authors based on [11]

Now, the prevailing demand is for applications on mobile devices and the use of a token or smart contract. However, SIM cards are currently being tested among several organizations. Based on the tests and research carried out, it will be possible to mitigate the shortcomings of the technology. And as a result, launch into mass production.

In the process of ensuring information security at VIC, certain problems may arise that could affect the company's activities. To prepare for them, potential risks were identified and, based on statistical and information analysis, the probability of their occurrence was assessed on a scale from 0 (extremely unlikely) to 1 (very likely). The risks were then ranked by the degree of impact on the company's activities and assessed on a scale from 0 (negligible) to 1 (significant). The obtained values were multiplied and displayed in an overall assessment presented in Table 1 on the summary risk map.

Table 1. Risk Assessment Card. Source: developed by the authors

Type of risk	Description	Consequences of the situation	Overall rating
Data leak	Leakage of confidential customer data and operational information	Damage to the company's reputation, fines and litigation	0.64
Cyber attacks	Deliberate actions by an attacker aimed at violating the availability, integrity or confidentiality of information	Loss of control over systems, theft of customer data, extortion, interruption of services and loss of finances	0.63
Technical threats	Viruses, malware, DDoS attacks	System disruption, data leakage, loss of control of infrastructure, network or company website downtime, loss of revenue and damage to reputation	0.56
Illegal access	Unauthorized access to company systems and data	Leakage of confidential information, secrets of business information, financial losses, disruption of competitiveness, damage to reputation	0.42
Internal human factor	Errors and lack of compliance with safety rules by employees	Data leakage, privacy violation and damage to company systems	0.35
Physical threats	Hacking of physical infrastructure, destruction of equipment, or access to secure company premises	Theft or destruction of equipment, access to confidential data, interruption of company operations	0.30
Failure to comply with rules and regulations	Failure to comply with legal and regulatory requirements in the field of information security and data protection	Regulatory fines, prosecution, loss of customer confidence and reputational damage	0.21
Social engineering	Manipulation of people, including deception, phishing and other forms of fraud	Information leakage, financial losses, threat to customer safety.	0.15
Investment losses	Excess of the amount of costs for a new technology compared to an already used one	Loss of funds	0.06
Financial losses	Loss of funds due to the inefficiency of the implemented system	Increased costs for fixing security bugs and decreased profits	0.04

The most significant risks are technical threats, data leaks and cyber-attacks. Physical threats and illegal access are rated as moderately significant risks, while social engineering, compliance with rules and regulations, and internal human factors are rated as risks of lower impact and likelihood compared to others. To mitigate the occurrence of risk situations, VIC should develop a comprehensive strategy and plans to ensure information security of information, including the introduction of appropriate technologies, personnel training,

establishment of policies and procedures, as well as regular monitoring and analysis of security systems.

The VIC information security system must be constantly updated, therefore, advanced technologies and progressive methods are required to ensure it. One of the key components of information security software at VIC is access control systems that allow you to determine and control the level of access to confidential information and company resources for employees, partners and clients using authentication, authorization and audit functionality. Access control systems may include two-factor authentication mechanisms, biometric scanning, or the use of smart cards to improve access security. Another equally important component is protection against external threats using intrusion detection and prevention software with systems that block unauthorized access attempts and promptly respond to abnormal activity in computer networks and systems. The most significant tools for ensuring information security are cryptography and encryption methods. Based on them, algorithms and methods are created to protect transmitted and stored data both in a branched organizational structure and on individual devices. However, using one tool does not allow achieving high results in protecting information, since there are various options for hacking and stealing it. This shows the need to set up a verification process for users with limited access to confidential information.

To maintain a high level of security and prevent hacking or theft of information, building protection only on the basis of reducing access to data and protection in the form of cryptography is not enough - it is necessary to supplement the protection with means of preventing attacks and identifying errors in the system. Using all information security tools together allows you to create a unified protection system and build a unified strategy on its basis and ensure the continuity of business processes.

Today in the Russian Federation, special attention is paid to the development of new cryptography and authentication tools in accordance with the requirements of information protection legislation and regulatory requirements in various industries. One of the most well-known cryptographic mechanisms is the electronic digital signature (hereinafter referred to as EDS), used as a replacement for classic passwords. The traditional tool for its implementation, used by most companies on the Russian market, are tokens, and the newer and more modern one is SIM cards. Although on the technical side both tools provide a high level of security and user authentication using cryptography and can be integrated with other systems and applications, the main economic advantage of SIM cards over tokens is the lower investment in installation. This is explained by the fact that in order to work correctly with tokens, additional resources are required to install special software on employee computers or mobile devices. And in the context of using a large number of tokens in the centralized infrastructure of the VIC, costs also increase. SIM card technology also has certain technical disadvantages when used in VIC. One of them includes the limited functionality of technological capabilities due to the specific nature of the company’s activities, which narrows the variability of authentication and data protection methods. However, both tools provide a high level of security and authentication and at the same time are limited in functionality. From a legal point of view, the use of both tokens and SIM cards imposes additional obligations on VIC to comply with the requirements of telecom operators, regulatory authorities and regulatory standards.

Today, SIM card technology continues to evolve to meet growing security requirements, while tokens stagnate and fail to deliver. To compare the mechanisms for working with tokens and SIM cards with digital signatures, let us turn to Figure 2, which provides a description of the steps and sequence of actions associated with the installation and use of tokens within the framework of information security in VIC.

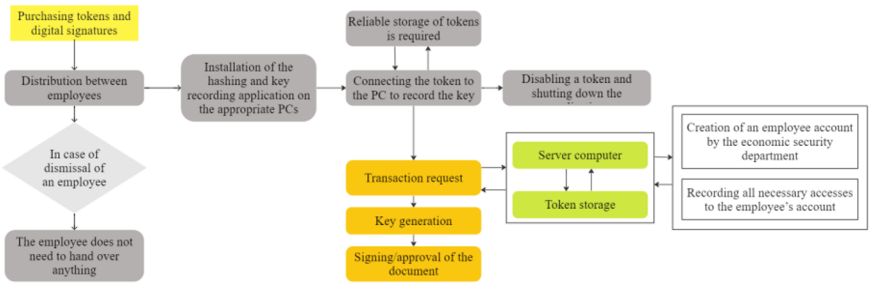

Fig. 2. Scheme of the process of installing tokens in the VIC business process. Source: developed by the authors

The first stage requires the acquisition of tokens and digital signatures and their physical distribution among employees who bear a high level of responsibility for them. To further work with tokens, a special application for hashing and using digital signatures is installed on users' personal computers, access to which will require a certain level of account access. At the next stage, if it is necessary to perform certain operations, the user connects a token, after which a request to perform the operation is made. To determine the user and his right to use a given token, the request is passed through the server storage and token storage, and after processing it, the data is hashed and a key is generated. Next, the document is signed and the token is physically disabled. Secure storage of tokens requires a place that is not susceptible to theft, since they are physically accessible and, despite the presence of a password, can be hacked.

Figure 3 demonstrates the sequence of steps required to successfully install and integrate SIM cards into the VIC for information security purposes.

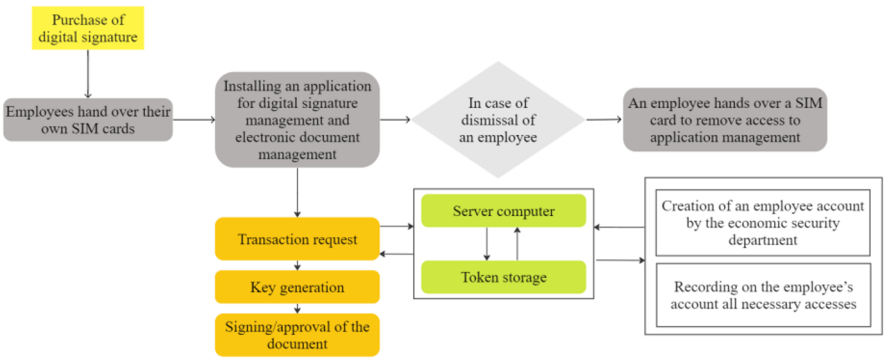

Fig. 3. Scheme of the process of installing SIM cards in the VIC business process. Source: developed by the authors

The procedure for using SIM cards includes their one-time purchase in the required quantity for employees and annual renewal of the digital signature. In this process, it is possible to procedurally purchase additional SIM cards for temporary use or expansion of the staff with the same level of access. At the first stage, employees hand over their SIM cards to be re-flashed so that they can use the application for working with the company's system. Then the digital signature management application is installed on mobile devices from the organization's website, application store or other resource. Then, without the need for tokens, users log in with their accounts and can submit transaction requests. When an employee leaves, the SIM cards are returned to the information security department and all data

associated with them is erased. The main advantage of using SIM card technology is the absence of physical contact and the ability to expand the functionality of the system to include processes for approving contracts, documents and other operations, which reduces risks and improves the efficiency of regulated processes in the company.

Note that in both cases, when receiving a request to perform an operation from a user, information about the user and the request itself pass through the servers and for its successful execution it is necessary to have information about the user in the system. Responsibility for entering and verifying information rests with the information security department, since if the user does not pass the necessary authorization, he will be denied installation of an electronic digital signature and access will be blocked. If the user is registered in the database and the information about him matches the requested one, a key will be generated to sign the document.

On the economic side, the process of replacing tokens with SIM cards requires certain financial resources to purchase the required number of SIM cards, applications for managing and updating digital signatures, ensuring reliable storage of SIM cards, training employees and introducing new procedures associated with the use of new technology. From a technical point of view, this process requires special applications for repurposing SIM cards to work with the company's infrastructure, mobile digital signature management, encryption and data exchange. In addition, it is necessary to ensure safe storage of SIM cards, technical support and, if necessary, system updates. From the legal side, the process of replacing tokens with SIM cards requires compliance with legislation regarding the use and storage of personal data of employees and clients of the company [4-7]. You should also take into account the requirements of regulatory authorities and ensure compliance with relevant regulations when replacing tokens with SIM cards. In addition, the VIC needs to develop and implement security policies that control access and use of SIM cards and the protection of sensitive data.

To successfully implement SIM cards with digital signatures into business processes and ensure their efficient operation, it is necessary that the organizational structure of the company meets certain requirements presented in Table 3.

Table 2. Requirements for the organizational structure for the implementation of authentication technology based on SIM cards with digital signature. Source: developed by the authors

Requirement	Description
Responsible person (group) or decision maker	The responsible person or group will be responsible for implementing the technology, developing strategy and coordinating the implementation and development of the authentication system
Ensuring information security	A group of people responsible for installing and maintaining authentication technology. The responsibilities of this group also include developing security policies
Training and retraining of employees	Personnel must be familiar with how the technology works, the authentication process, and safety precautions. There should be refresher courses if the technology improves or if the employee is not familiar enough with the technology
Maintaining the system in working order	It is necessary to have a support service in case of system failures, as well as for its maintenance.
Development and creation of a security policy	Implementation of an official document within the organization, including rules for working with data and an authentication system

Data monitoring and audit	Development of mechanisms for monitoring and analyzing the authentication system for failures and tracking the operation of the system in accordance with the established algorithm
Data quality	Development of mechanisms that control errors in the operation of the system in order to identify, correct and prevent them, as well as to record and correct anomalous cases
Legal Compliance	Meeting legal and regulatory requirements regarding authentication and information security
Well-established communication among employees and departments	In addition to training employees, well-established communication between them is required in order to prevent errors and perform the necessary tasks when using the system
Updating and improving the system	Avoiding hacking threats by updating the system and updating it

Note that VIC already has an organizational structure that fulfills the described necessary requirements for the effective implementation of SIM card technology with digital signature. If companies with different organizational structures plan to implement this technology and work effectively with it, they need to either organize a similar structure or combine a number of requirements into groups in order to fulfill the basic conditions associated with the implementation and support of such technology.

6 Conclusions

Based on the study, we can conclude that VICs require a specific approach to ensuring information security, and the assessment and analysis of company risks showed that the most important threats are technical vulnerabilities, data leaks and cyber-attacks. An important limitation of the use of this technology is the cryptographic method of encrypting information. Due to this method, SIM cards cannot be used abroad.

During the analysis of modern methods and tools for ensuring VIC information security, the main attention was paid to authentication technology based on tokens and SIM cards with digital signature. It was determined that the use of SIM cards represents a promising alternative to tokens. For successful implementation of technology, it is necessary that the company's organizational structure meets certain requirements and has the necessary financial, technical and legal resources aimed at acquiring technology, applications for managing digital signatures, ensuring its secure storage, updating the system, complying with regulatory requirements and developing a security policy for access control and protection of confidential data. The listed aspects are carried out in VIC, which makes it possible to successfully implement an authentication system based on SIM cards with digital signature.

The theoretical significance of the results lies in expanding knowledge about the features, structure, requirements and risks of ensuring information security in the VIC. The study allows us to study the advantages and limitations of tokens with digital signatures in comparison with SIM card technology, understand the scheme for introducing them into the company’s activities and determine the requirements for the success of this process. The practical significance is that VIC offers a new tool to ensure a high level of security and authentication. Providing this tool will satisfy the needs of organizations in protecting information, which in the future can serve as the basis for the mass dissemination of technology. The theoretical and practical results obtained can be useful for researchers, technical specialists, regulatory authorities, normative organizations and representatives of VIC and can serve as the basis for further scientific work, the creation of specific methods

and tools for effective protection of VIC systems, and the development of appropriate regulatory standards for the use of SIM cards with digital signature.

References

1. Al Mousa A. Utilizing the eSIM for Public Key Cryptography: a Network Security Solution for 6G /A. Al Mousa, M. Al Qomri, S. Al Hajri, R. Zagrouba // 2nd International Conference on Computer and Information Sciences. 2020. Electronic resource: https://clck.ru/374ZUC
2. Antokhin Yu.N. Improving business processes in a company / Yu.N. Antokhin, K.A. Gladeeva // Economics. Right. Innovation. 2019. No. 4. pp. 61-71
3. Biryukova V.V. Effectiveness of development of vertically-integrated oil companies based on the use of strategic advantages: dis. for the academic degree of Dr. econ. Sciences: 08.00.05 / V.V. Biryukova. 2021. P. 336
4. «Criminal Code of the Russian Federation» dated June 13, 1996 No. 63. Electronic resource: https://clck.ru/hS8Je
5. Federal Law «On Advertising» dated March 13, 2006 No.38. Electronic resource: https://clck.ru/bNGs6
6. Federal Law «On Information, Information Technologies and Information Protection» dated July 27, 2006 No.149. Electronic resource: https://clck.ru/ggWjK (in Russ)
7. Federal Law «On Personal Data» dated July 27, 2006 No.152. Electronic resource: https://clck.ru/gLnFq
8. Kremer F. Cyber risk and cybersecurity: a systematic review of data availability / F. Kremer, B. Sheehan, M. Fortmann, A.N. Kia, M. Mullins, F. Murphy, S. Matern // Geneva PAP risk insurance practice. 2022. Vol. 47(3). pp. 698-736. doi: 10.1057/s41288-022-00266-6
9. Matveev A.V. Features of internal control of vertically integrated structures of oil and gas industry enterprises / A.V. Matveev, M.S. Shatsky // Modern aspects of accounting, analysis and audit: Materials of the Regional Scientific and Practical Conference, Krasnoyarsk, November 15, 2018 / Chief Editor G.I. Zolotareva. – Krasnoyarsk: Federal State Budgetary Educational Institution of Higher Education «Siberian State University of Science and Technology named after Academician MF Reshetneva». 2018. pp. 62-64
10. Mishra A. Attributes impacting cybersecurity policy development: An evidence from seven nations / Alzoubi YI, Anwar MJ, Gill AQ // Computers & Security. 2022. Vol. 120. Electronic resource: https://clck.ru/374ZVE
11. Nadeikina V.S., Lagutkina T.V. ANALYSIS OF METHODS FOR IMPLEMENTING A MULTIFACTOR AUTHENTICATION SYSTEM // Scientific result. Information Technology. 2022. No. 4. URL: https://cyberleninka.ru/article/n/analiz-sposobov-realizatsii-sistemy-mnogofaktornoy-autentifikatsii (date of access: 02/28/2024).
12. Nosova E.A. Information security system in ensuring economic security and risk management at an enterprise / E.A. Nosova, L.V. Anisimova, T.S. Murovana, Yu.A. Svyatiuk, E.R. Yafinovich // Proceedings on ensuring cybersecurity in information and telecommunications media. Vol. 2. 2021. pp. 21-31
13. Okumbekova M. Nature of “vertical integration” and features of management in these structures / M. Okumbekova // Moscow Economic Journal. 2021. No. 12. pp. 577-585

14. Subbotin A.S. Issues of information security of vertically integrated oil companies in conditions of digitization / A.S. Subbotin // Creative Economy. 2021. Vol. 15(12). pp. 5005-5014. doi: 10.18334/se.15.12.114004
15. Sukhmeetsingh G. ESIM Mechanism / G. Sukhmeetsingh // International Journal of Scientific Research in Computer Science Engineering and Information Technology. 2021. Vol 7(2). P. 1-4. doi: 10.32628/cseit21721
16. Surabhi T. ESIM on IoT: An Innovative Approach Towards Connectivity / T. Surabhi // International Journal of Engineering Research & Technology. 2020. Vol. 8(5). P. 1-4. doi: 10.17577/IJERTCONV8IS05053
17. Tan G.T. Challenges of Post-Quantum Digital Signing in Real-world Applications: A Survey / P. Szalachowski, J. Zhou. International Journal of Information Security. 2019. Electronic resource: https://eprint.iacr.org/2019/1374
18. Topoleva T.N. The role of vertically integrated structures in the development of the production sector of the economy / T.N. Topoleva // Issues of regional economics. 2019. No. 2(39). pp. 81-89
19. Zhukovskaya I.E. Modern trends in the development of information security tools in information systems / I.E. Zhukovskaya // BI technologies and corporate information systems in business process optimization: Proceedings of the VII International Scientific and Practical Conference, Yekaterinburg, November 27, 2019 / Responsible. for the release of D.M. Nazarov, S.V. Begicheva, E.V. Zubkova. Ekaterinburg: Ural State Economic University, 2020. pp. 28-30.