International Journal of Advanced Engineering and Management Research

Vol. 9, No. 05; 2024

ISSN: 2456-3676

Development of a Universal Platform for Managing Payment Operations on a Global Scale: Methodology and Implementation Examples

Asha Seshagiri[1]
[1]Software Development Engineer 3 at Expedia
JSS Academy of Technical Education at VTU
(Visvesvaraya Technological University),
Bangalore, Karnataka, India

doi.org/10.51505/ijaemr.2024.9505 URL: http://dx.doi.org/10.51505/ijaemr.2024.9505

Received: July 28, 2024 Accepted: Aug 08, 2024 Online Published: Oct 05, 2024

Abstract

The article discusses the main trends and processes in the field of digital finance. The purpose of the research is to analyze the functioning of electronic payment systems as a key element of the digital financial sector, with a focus on identifying the main threats to user security and developing recommendations to improve their security. The author analyzes the functioning of electronic payment systems as an important segment of the digital finance sector. Statistics on the global electronic payments market and forecast indicators are presented. Main security issues for users of electronic payment systems are listed and described. It is noted that customers conducting transactions through an electronic payment system have to disclose some personal and financial information, which exposes them to the risk of data leakage. The use of electronic payment systems is associated with several risks, which vary depending on technology, provider company, and user awareness. A list of major risks is presented, focusing on the stage of authorization and authentication of the client within the system. Ways, methods, and technologies to enhance client security during entry into the payment system, as well as main methods of ensuring security (secure Internet connection, client identification and access control, technical protection, payment system certification), are discussed. Advantages and disadvantages of password-based technologies are presented, including one-time passwords (OTPs), single sign-ons (SSOs), OAuth, OpenIDs, One Identity, and One Key, and the Cyber Source platform.

Keywords: transaction, electronic payment system, digitization, digital finance, passwordless access, OTP (one-time password), cyber source, one key, one identity, security token, authorization and authentication.

Introduction

Digital finance has certainly become the most important transformative factor for the global economy. It has dramatically changed how individuals, governments, foreign traders and enterprises interact, and the concept of "digital finance" encompasses a wide range of technologies, processes and products, from mobile payments and online banking to crypto currencies and block chain technology [5, p. 593]. This transformative power is fueled by its ability to enhance efficiency, reduce costs, and expand access to financial services, particularly in underserved regions. As a result, digital finance is rapidly reshaping the global financial landscape, challenging traditional institutions and creating new opportunities for innovation and growth.

However, this rapid evolution also presents significant challenges. Concerns regarding data privacy, cyber security, and the potential for financial instability are emerging as key areas for consideration. This research will explore the intricate interplay between the opportunities and challenges presented by digital finance, focusing on the vital role of electronic payment systems and their impact on user security.

The relevance of the research. The degree of scientific development of the topic. Despite the high dynamics of the digital finance sector's development, problems, risks and barriers are increasingly present. However, the pace of development in this field is so fast that not all aspects are studied by the scientific community. Foreign and domestic research is mainly focused on specific aspects of digital finance, such as programming and business administration. There is a lack of research that provides an analytical and generalized interpretation of social problems. This is complicated by the interdisciplinary nature of research, which is carried out at the intersection of different fields, such as finance, economics, and programming.

The most controversial and urgent issue is cybersecurity - maintenance of the sensitivity of personal and corporate data, control of cyber fraud, financial crime prevention and prevention of situations that cause reputational damage to financial institutions, businesses and governments.

The theoretical and practical significance of the article. This study has significant theoretical and practical value, making a significant contribution to the development of scientific discourse in the field of digital finance and information security. The theoretical significance of the study lies in the systematization and deepening of understanding of the functioning of electronic payment systems as an integral part of the digital financial landscape. The study analyzes the main trends, processes, and challenges associated with the development of electronic payments, including security issues, and offers a deep analysis of the risks faced by users of these systems. The practical relevance of the study is in the development of specific recommendations for improving the security of users of electronic payment systems. The study proposes practical mechanisms and technologies to enhance the protection of customer information during authorization and authentication in systems, including the use of one-time passwords, single sign-on systems, OAuth, OpenID, One Identity, One Key and the CyberSource platform. The results of the study can be used to both improve the practice of electronic payment systems and form more effective regulatory mechanisms in this area to ensure security and user trust.

Research design. The requirement to achieve this goal led to a consistent study of scientific publications by Russian and foreign authors, as well as corporate websites of technology developers in the field of FinTech. Statistical, reference, and methodological literature was also used. While the article was being written, general scientific and specific methods of scientific research were applied, such as systematization, analysis, comparison, and graphic interpretation.

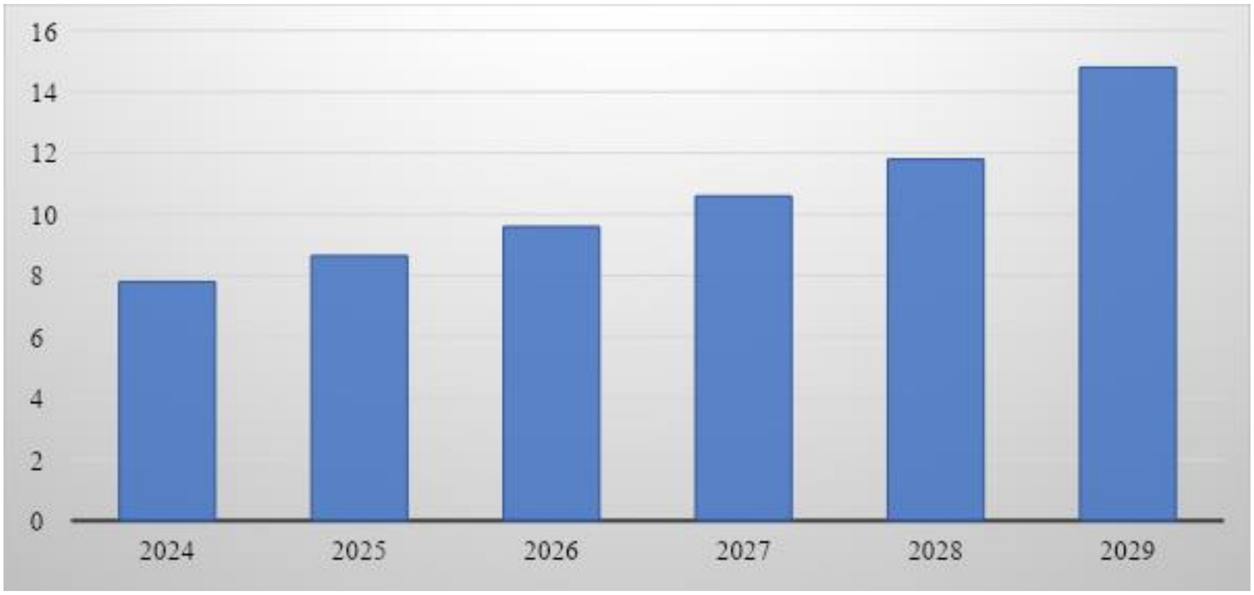
Digitalization of the financial sector and its consequences. As a rule, structures involved in the field of digital finance face a universal set of risks inherent to any digital system within which financial flows circulate. This includes a centralized approach to the accumulation of financial and personal information, making the task of attackers easier, limiting the circle of persons carrying out cross-border transactions, including due to sanctions, and the opacity of activities of electronic systems, resulting in the impossibility of operational control and audit of the operators of international electronic systems [2, p. 194]. Experts also point out risks such as technical failures in financial transactions, a constant increase in cyber-attacks, and the emergence of new types of cybercrime targeting funds [13]. Negative aspects of the digital financial market include commissions (including hidden ones), delays in transactions, increased use of intermediaries for settlement and payment, and increased abuse of office positions by responsible parties, including selling [2, p. 195].

Electronic payments are an important segment of the digital finance sector. The key structure of this sub-industry is the electronic payment system - transactions are carried out via this digital settlement system. Financial information in such a system circulates through network channels, which eliminates the need for manual processing of traditional payment orders.

Electronic payments can be made through banking payment systems such as Visa, MasterCard, Mir, as well as through interbank settlement systems via electronic communication channels and through so-called "fast payments" made by banks using phone numbers. A new stage in the evolution of electronic payments is represented by "electronic wallets" and non-bank payment systems. Additionally, digital payment elements are about to be integrated into non-financial sectors, such as payments in messengers (for example, Chinese WeChat) and social networks (paid "gifts", premium subscriptions, etc.) as part of the mobile operator's infrastructure and other means.

Every year, the national statistical offices of most countries notice an increase in the volume of electronic payments. This trend can be explained in many ways: the reduction in the cost of smart devices, their increased availability to the general public, the increase in internet coverage, and the increase in the digital literacy level of citizens. Electronic payments have become a part of everyday life not only for individuals, but also for businesses. The effectiveness of technology transfer in promoting organizational change within the electronic payment sector is also a crucial factor for its success [11].

The global digital payments market was valued at $7.79 trillion in 2023. Projected CAGR from 2024 to 2029 is 11.08% and will reach $14.77 trillion by 2029 (Picture1):



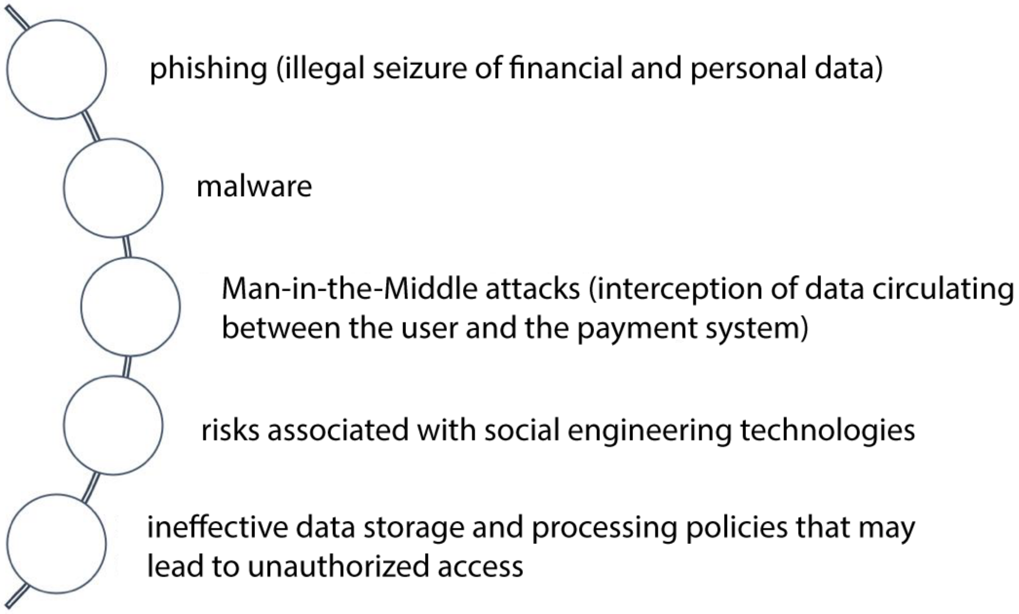
Picture 1. Dynamics of the global electronic payments market, trillion US dollars, 2024-2029. *Note:* source – own development based on data [7]

Problematic aspects of ensuring security in electronic payment systems. Taking into consideration the enormous size of the global electronic payment market, security issues for its participants become more prominent. The need for security of electronic payments is essential for all parties involved in the payment system. Consumers who make transactions should be confident in the protection of their funds and personal data, while sellers should be assured of smooth operation of the payment system when selling goods and services. Financial institutions must protect and only process voluntary and legitimate transactions. They also need tools to track and detect suspicious payments [9]. The state represented by legislative and executive bodies is interested in uninterrupted and efficient operation of electronic payment systems. Analysis of foreign and domestic legislation in this area reveals that the state typically requires payment systems and financial intermediaries to provide information to clients about transaction conditions, such as commission rates, collection procedures, exchange rates, payment delivery times, terms for accepting or rejecting payments, and so on.

When working with an electronic payment system, users conducting transactions are required to provide some personal and financial information - these are the minimum requirements for being included in the list of authorized users. Consequently, clients consciously expose themselves to the risks associated with data leakage.

Hence, payment systems, their operators, and intermediaries at various levels introduce all kinds of anti-fraud mechanisms into their electronic interfaces and internal infrastructure. An anti-fraud system, from the English fraud, can be defined as a set of actions and tools aimed at monitoring and preventing illegal financial actions in real time, as well as managing clients and assessing the degree of risk [3, p. 152]. Research indicates the importance of advanced machine learning techniques in developing robust fraud detection systems for credit card transactions and online payments [12, 14, 15].

Thus, the use of electronic payment systems involves a number of risks, which may vary depending on the technology, the provider company, and the level of user awareness. Let's imagine the main risks that a client may face (Picture 2):


phishing (illegal seizure of financial and personal data)
malware
Man-in-the-Middle attacks (interception of data circulating between the user and the payment system)
risks associated with social engineering technologies
ineffective data storage and processing policies that may lead to unauthorized access

Picture 2. Risks when using electronic payment systems. *Note:* source - own development

Awareness of these risks is a key condition for minimizing threats and protecting funds and personal information when using electronic payment systems. At the same time, the payment service provider bears a significant share of responsibility for neutralizing risks. The stability of the payment system largely depends on the state of the infrastructure provided by the provider. It should be noted that one of the most "sensitive" stages of working with an electronic payment system is the client log-in phase. A significant proportion of anti-fraud tools is used to increase security during the authorization phase. Fine-grained co-occurrence analysis of user behavior can be instrumental in enhancing fraud detection capabilities in online payment systems [10].

Ways, methods and technologies aimed at increasing client security when entering the payment system. The developer of an electronic payment system faces the challenge of balancing the need to ensure the security of login and the ability to use different login methods. At present, there are several main ways to ensure security in the development of payment systems (Table 1):

Table 1. Basic methods (directions) for ensuring the security of electronic payment systems. *Note:* source – own development using data [1]

Direction	**Contents of measures**
Secure (encrypted) Internet connection	Encryption of the Internet connection is achieved through an SSL certificate on the site, as well as other measures certified in accordance with international standards.
Measures to identify the client and limit unauthorized access	System for entering a login and password to access the system, password testing for complexity; passwordless access systems (see below); a combination of a bank card number, expiry date, cardholder's name, CVV/CVC codes; virtual cards issued specifically for online payments (ensuring the security of the customer's main card).
Technical protection measures	Linking the payment service to a fixed IP address and telephone number, providing client access to the system via an encrypted HTTPS/SSL protocol, a virtual keyboard for data entry, and separation of transaction creation channels and transaction authorisation channels through a special code sent via SMS.
Certification of payment systems	Certification of service providers and business owners (sellers), Qualified Security Assessor (QSA) certification according to the Payment Card Industry Data Security Standard (PCI DSS), ISO/IEC 27001:2005 certification, etc.

Rejection of password access vs. security of the client of the electronic payment system. Many payment systems implement passwordless authorization systems. A password, on the one hand, increases the level of client security and acts as an additional "filter" for logging into the system. However, on the other hand, it is a weak point in the security system, and is not convenient for users. In particular, a password should not be repeated on other services, and should be complex. However, passwords are difficult to remember and users often write them down on paper or electronic devices.

Passwordless authorization partly allows you to neutralize such risks. In discussions on the topic of passwords for entering electronic payment systems, there is still no unanimity of opinion: according to some experts, the only correct and adequate solution for modern realities is two-factor authentication (2FA), while others point out the advisability of abolishing passwords altogether.

The first attempts to abandon passwords for authentication were made in the 1980s: the new technology was called one-time password (OTP). A one-time password, as a rule, is a numeric code 4-12 characters long which is sent to the client via SMS, push notification, email, or as part of the client's phone number. In addition, mobile apps (Google Authenticator) and payment services can generate and send these codes after authorization.

In the next decade, SSO technology was developed, which made it possible to authenticate users on multiple sites and applications using a single set of registration data. This technology has been significantly modified since then and continues to be used in modern systems today.

Among the "single sign-on" technologies, OAuth and OpenID should be noted - thanks to them, the client can authenticate in the electronic payment system using a single account without entering a password. In practice, a user's account on social networks is most often used. Thus, when authenticating, the payment system's client does not need to enter a combination of a login and a password, but rather an access token provided by OAuth or OpenID. Similarly, cross-authentication works on mobile devices - a client logging into social networks on a phone eliminates the need for authentication in another application using OAuth technology. Several alternative passwordless login options are available on the market, such as the One Identity system, which is a comprehensive identity and access management (IAM) platform designed to simplify authentication, authorization, and management of user accounts in electronic environments [8].

One Identity presents a comprehensive solution [8] to the intricate challenge of identity management within a rapidly evolving and increasingly complex digital landscape. The platform addresses the growing complexity of identity security in an era marked by the exponential proliferation of human and machine identities and the ubiquitous shift to cloud-based operations and the widespread adoption of remote working. One Identity addresses this challenge by providing a unified set of solutions covering the four pillars of identity security: identity governance and administration (IGA), access management (AM), privileged access management (PAM) and active directory management (AD Mgmt) [8]. This integrated approach meets the critical need for a comprehensive security strategy in a fragmented environment, offering unmatched visibility, control and protection against a variety of evolving threats. The platform's modularity and connectivity allow for seamless integration with existing IT systems and security solutions, enabling organizations to tailor their identity security strategy to their specific operational needs. This flexibility is further enhanced by an increasing number of integrations with leading industry systems and platforms, optimizing identity security throughout an organization's entire technological landscape.

One Identity allows you to manage accounts and access them, thanks to features such as passwords and social logins [8]. Thanks to the password management feature, users can independently reset their passwords using identity verification methods such as answering security questions and multi-factor authentication. The One Identity platform also allows you to synchronize passwords across different systems and apps, providing a single login for multiple accounts, making it easier to manage your credentials. Integration with social media is a key advantage of One Identity, as the technology supports social media authentication, allowing users to log in to payment systems using their social media accounts. Additionally, One Identity automates the creation and deletion of accounts in payment systems based on data received from social media.

In doing so, One Identity's comprehensive approach goes beyond security to deliver tangible benefits in the form of increased operational efficiency, cost savings, and risk mitigation. The Unified Identity Platform enables organizations to transition from reactive and fragmented security strategies to proactive and holistic solutions, resulting in a more robust and secure environment. This shift allows organizations to operate with greater confidence and agility in the face of emerging threats and constant technological evolution. One Identity bridges the gap between traditional security frameworks and the demands of a dynamic digital world, empowering organizations to navigate identity security complexities while mitigating risks associated with fragmented approaches.

One Key presents another sophisticated approach to identity management, prioritizing both security and the user experience [16]. The platform leverages advanced cryptographic algorithms to securely store and manage passwords and other sensitive credentials within an encrypted environment, minimizing the risk of unauthorized access and data breaches [16]. The integration of advanced cryptographic techniques ensures the integrity and confidentiality of user data, providing a robust layer of protection against malicious actors, emphasizing its application in the secure management of digital assets, especially in the context of cryptocurrency wallets [16]. One Key's Auto-Fill feature streamlines the authentication process by automating the filling of password fields, significantly reducing the risk of phishing attacks and enhancing the user experience [16]. This feature not only simplifies logins but also mitigates the potential for human error often associated with manual password entry.

One Key embraces a multi-layered approach to authentication, supporting a diverse range of methods, including SMS codes, time-based one-time password (TOTP) generation, biometric authentication, and hardware token integration [16]. This comprehensive approach provides users with flexible and secure authentication options tailored to their individual security preferences and technological capabilities. Furthermore, One Key facilitates unified authentication across multiple systems, allowing users to access diverse applications and platforms using a single login process and interface [16]. This streamlined access management simplifies the user experience, minimizing the need for multiple passwords and accounts.

One Key seamlessly integrates with social networks through the utilization of industry-standard protocols such as OAuth and OpenID, enabling users to leverage their existing social media accounts for secure and convenient logins [16]. This integration not only simplifies the authentication process but also provides a layer of social verification, enhancing the overall security posture of the platform.

One should also take a closer look at CyberSource, a comprehensive e-commerce platform that allows you to manage transactions, prevent fraud and ensure the security of payments and customer data. Developers and owners of electronic payment systems can easily integrate CyberSource: the platform provides APIs and ready-made integration modules for online stores and payment systems to integrate with existing interfaces and websites. CyberSource also allows you to use credit and debit cards, e-wallets, bank transfers, and alternative payment methods.

The CyberSource platform uses machine learning algorithms and Big Data analysis to identify and prevent fraudulent transactions. CyberSource analyzes a user's behavior, transaction history and typical patterns, as well as other parameters, to identify potential threats. In addition, CyberSource ensures the protection of customer data by using modern 3D Secure encryption and tokenization techniques in accordance with the Payment Card Industry Data Security Standard (PCI DSS) [6].

The analysis of the presented One Identity, One Key and CyberSource platforms demonstrates that a new approach combining advanced technology, data privacy and adaptation to changing user needs is required to achieve optimal security and usability in electronic payments. The managerial perspective of this analysis emphasizes the need to implement a strategy based on the integration of different solutions. The introduction of platforms like One Identity and One Key, which provide unified management of accounts, passwords, and support authentication through social media, helps improve user experience and create a single, centralized security mechanism. Implementing solutions like CyberSource, using machine learning and big data analytics to detect and prevent fraud, enables proactive response to new threats and minimizes risk. Importantly, compliance with data security standards such as PCI DSS is integral to building trust in electronic payment services. This comprehensive approach, which includes not only technical solutions but also attention to improving the level of cyber literacy of users, will help create a safer and more efficient environment for online payments.

The conclusions

Thus, the conducted study allows us to draw the following conclusions:

- Electronic payments are the most important segment of the digital finance sector. An electronic payment system is a digital settlement system through which transactions are carried out. Electronic payments can be made via the Visa, Mastercard, Mir payment systems, as well as through interbank settlement systems, fast payments, electronic wallets, and non-bank payment systems.
- Considering the growth dynamics of the global electronic payment market, security issues for its participants come to the fore. The use of electronic payment systems involves a number of risks, which may vary depending on the technology, the provider company, and the level of the user's digital literacy.
- When working with an electronic payment system, people carrying out transactions are forced to provide personal and financial information about themselves. Thus, they consciously expose themselves to risks associated with data leakage. One of the most "sensitive" stages of working with a payment system is the login phase, so a significant amount of anti-fraud technology is aimed at enhancing security during authorization.
- The developer of an electronic payment system faces the challenge of balancing the need to ensure the security of logins with the ability to use various login methods. In the current practice of developing payment systems, the following are the main ways to ensure security: secure (encrypted) internet connections, measures to verify the identity of the client and prevent unauthorized access, and technical protection measures. Certification of payment systems is also used to ensure their reliability.

- Modern payment systems increasingly introduce passwordless authentication systems. One such technology is a one-time password, a numeric code 4-12 characters long that is sent to the customer via SMS, push notifications, or email. Another technology is the single sign-on (SSO). This method allows users to authenticate on multiple websites and applications using a single set of login credentials. SSO solutions include OAuth and OpenID, and there are many "single sign-on" solutions available on the market, such as One Identity, OneKey, CyberSource, and others.

In addition, research conducted to analyze the functioning of electronic payment systems in the context of a rapidly developing digital economy revealed a number of key issues related to user security. In particular, analysis showed that traditional password-based authentication models are not always able to adequately counter modern cyber threats, especially in light of increasing complexity and sophistication in attackers' methods.

The study revealed the need for comprehensive security measures, including not only traditional methods such as data encryption and multi-factor authentication but also new technologies to improve security. These include passwordless authentication, biometric identification systems and machine learning for fraud prevention. Active participation in ensuring user security is also crucial, including the development of digital education and increasing cyber literacy among the population.

This study emphasizes the need for continuous improvement of security mechanisms in the field of electronic payments. Further research should aim to analyze the effectiveness of new security technologies, study new threats, and adapt security measures to changing conditions. It should also develop a legislative framework for regulating security in electronic payments. Implementation of the recommendations obtained will ensure sustainable growth in the electronic payments market and build trust in digital financial services.

The survey results call for a more proactive and comprehensive information security risk management strategy for digital finance organizations. The key factor is not only technological development, but also increasing cyber literacy among users. This involves developing educational programs, raising awareness of threats, and promoting safe practices in digital services. It is also important to ensure close cooperation between organizations working in the field of electronic payments, regulators, and research institutes to create an effective system of protection and response to cyber threats.

References

Security of electronic payments. – 2024 [Electronic resource]. – Access mode: http://pay2.ru/payment-security/. – Access date: 07/03/2024.

Dyudikova, E. I. Models of integration of digital technologies into the international payment space / E. I. Dyudikova // π-Economy. – 2020. – No. 3. – pp. 187-200.

Kopnin, A. A. Methodology for ensuring the security of banking Internet transactions based on antifraud systems / A. A. Kopnin, E. V. Sokolova, A. A. Dolgopolov // International journal of professional science. – 2022. – No. 10. – pp. 149-157.

Minakov, A. V. Analysis of risks and security of the electronic payment system / A. V. Minakov, N. D. Eriashvili // Education. The science. Scientific personnel. – 2024. – No. 1. – pp. 274-281.

Khodzhaev, A. Digital finance: trends, challenges and prospects in the context of modern economics / A. Khodzhaev, G. Maksadov, Ya. Meredova // World scientist. – 2024. – No. 24. – pp. 591-598.

Cybersource. – 2024 [Electronic resource]. – Access mode: https://www.cybersource.com/en.html. – Access date: 07/03/2024.

Digital Payment Market Report 2024-2029 // Mordor Intelligence – 2024 [Electronic resource]. – Access mode: https://www.mordorintelligence.com/ru/industry-reports/digital-payments-market. – Access date: 07/03/2024.

One Identity Password Manager. – 2024 [Electronic resource]. – Access mode: https://roi4cio.com/catalog/product/one-identity-password-manager. – Access date: 07/03/2024.

Wang C. CAeSaR: An online payment anti-fraud integration system with decision explainability / C. Wang, S. Chai, H. Zhu, C. Jiang // IEEE Trans. Dependable Secure Comput. – 2023. – No. 3. – pp. 2565-2577.

Wang C. Representing fine-grained co-occurrences for behavior-based fraud detection in online payment services / C. Wang, H. Zhu // IEEE Trans. Dependable Secure Comput. – 2022. – No. 1. – pp. 301-315.

Lavoie J. R. Technology transfer evaluation: Driving organizational changes through a hierarchical scoring model / J. R. Lavoie, T. Daim, E. G. Carayannis // IEEE Trans. Eng. Manage. – 2022. – No. 6. – pp. 3392-3406.

Aburbeian A. M. Credit card fraud detection using enhanced random forest classifier for imbalanced data / A. M. Aburbeian, H. I. Ashqar // Proc. Int. Conf. Adv. Comput. Res. – 2023. – pp. 605-616.

Alghamdi S. Technology Assessment for Cybersecurity Organizational Readiness: Case of Airlines Sector and Electronic Payment / S. Alghamdi T. Daim, S. Alzahrani // IEEE Transactions on Engineering Management. – 2024. – vol. 71 – pp. 7701-7718.

Malik E. F. Credit card fraud detection using a new hybrid machine learning architecture / E. F. Malik, K. W. Khaw, B. Belaton, W. P. Wong and X. Chew // Mathematics. – 2022. – No. 9 – p. 1480.

Gupta K. Machine learning based credit card fraud detection. A review / K. Gupta, K. Singh, G. V. Singh, M. Hassan, G. Himani, U. Sharma // roc. Int. Conf. Appl. Artif. Intell. Comput. (ICAAIC). – 2022. – pp. 362-368.