Ingénierie des Systèmes d'Information
Vol. 29, No. 2, April, 2024, pp. 523-532
Journal homepage: http://iieta.org/journals/isi

Innovative Technologies as a Factor of Information Security of the Republic of Kazakhstan

Kuralay Azanbay

Department of Information Systems, Al-Farabi Kazakh National University, Almaty 050040, Republic of Kazakhstan

Corresponding Author Email: kuralayazanbay@yahoo.com

https://doi.org/10.18280/isi.290213

Received: 10 August 2023
Revised: 3 November 2023
Accepted: 12 March 2024
Available online: 25 April 2024

Keywords:
data protection, information security, automated processes, technological innovation, digital economy, advanced systems, Kazakhstan

ABSTRACT

The introduction of innovative technologies is essential for ensuring information security in Kazakhstan. This research aimed to determine the main success factors for applying innovative technologies to guarantee reliable information protection in Kazakhstan. The methodological approach combined system analysis of Kazakhstan's information security legislation with empirical modeling of key principles for developing and implementing technological innovations. The results showed that Kazakhstan's government supports technological innovations in information security through regulations and programs like "Digital Kazakhstan." However, challenges exist due to underdeveloped digital infrastructure. Threats to information security in Kazakhstan include multi-ethnic tensions, media dependence on commercial entities, a lack of a domestic electronics industry, and the erosion of cultural values. Effective innovations include integrated circuits, high-tech components, virtual client protection, enterprise network support, big data analytics, improved cloud security, and container security. Their benefits over conventional systems include better resource efficiency, scaled capacity, accelerated development, improved responsiveness, and innovation. Recommended innovations for Kazakhstan include protecting virtual clients, supporting corporate network deployment, leveraging big data, advancing container security, and boosting cloud technologies.

1. INTRODUCTION

The problematics of this scientific research are determined by the essential importance of technological innovations in the sphere of information security in Kazakhstan and the necessity to establish and implement a new approach to the issues of information protection. Currently, the Republic of Kazakhstan is vulnerable in this aspect, as it belongs to the developing countries that have transitioned to the "information age" without completing the mandatory stage of development of agrarian and industrial society. It explains some difficulties in the implementation of innovative technologies in the field of information protection, which are occurring in the country at the moment. Nowadays, Kazakhstan has an insufficiently developed digital infrastructure, which causes difficulties in mastering innovative technological solutions that ensure the achievement of an appropriate level of information protection for individual enterprises or individuals. In addition, there are specific difficulties in attracting investment in the development of innovative projects of this kind [1]. Innovations in the field of information security, as a rule, have high costs, which, against the background of insufficient state support, causes specific difficulties in their development and implementation. Nevertheless, innovative technologies of this kind are extremely relevant for the economy of Kazakhstan, as they allow for an increase the level of protection of personal data of citizens and organisations in virtually all spheres of society.

The research team consistsing of Erzhinbek et al. [2], in their scientific research, considered several problematic aspects of the evolution of innovative technologies and principles of information protection in the sphere of higher education in Kazakhstan. The researchers note that one of the key objectives of the state program "Digital Kazakhstan" is the introduction of digital technologies in various spheres of society and the establishment of conditions for the development of the digital economy. The authors highlight the importance of information security within Kazakhstan's digital transformation, as ethical issues arise with greater access to information. For its part, Polomarchuk [3], in scientific research on the problems of ensuring information security in the Republic of Kazakhstan, notes that the development of the current society has entered the information age. Particular importance in this context, according to the researcher, is information security, as the problems of "ethical collapse" in the information sphere in the conditions of the formation of the information society have acquired significant relevance. The introduction of innovative technologies in the field of information protection should provide a successful solution to this problem.

In turn, Sabitov [4], who considered several problematic aspects of information security in Kazakhstan in his research, notes the fact that the concept of information security is adopted in the country at the state level. Therewith, the author notes that in this context, the emphasis is on the technical side of the problem. From this standpoint, the current state of

information security in the country is assessed by the presence of some threats that can be levelled by introducing a set of innovative technologies. Therewith, a team of researchers consisting of Pirounias et al. [5], in a joint research work designed to explore the relationship between information security issues within a single enterprise and the market value of its assets, note that investment in the establishment of innovative technologies for information security is currently one of the key expenditure items of government budgets in several countries. According to scientists, in recent years in the field of corporate governance, there has been a shift in emphasis towards strengthening information security and enhancing database protection through the introduction of various kinds of technological innovations. Sabitov [4] and Pirounias et al. [5] demonstrate the emphasis that has been placed on the technical aspects of information security threats and the significant costs associated with innovative security technologies. A group of scientists comprising Saglam et al. [6] examined several problematic aspects of ensuring the protection of personal data through technological innovation. The researchers concluded that modern advances in information technology have significantly improved the quality of personal data protection. It is noted that using innovative technologies to protect personal data and ensure the information security of enterprises and individuals should be regulated at the legislative level.

While these studies have explored problematic aspects and ethical dilemmas surrounding information security, less focus has been placed on determining the specific factors that contribute to successfully implementing innovative technologies for information protection in Kazakhstan. This research aims to build on the existing literature by identifying the key factors, across technological, economic, and regulatory dimensions, that enable the effective adoption of information security innovations within the Kazakhstani context. The end goal is to provide practical recommendations for how Kazakhstan can improve its approach to information protection as it continues to develop its digital infrastructure and economy. Examining what drives successful adoption of these technologies can help bridge the gap between innovation and implementation.

The main purpose of this research is to determine the main factors of success of the application of innovative technologies to ensure reliable protection of information, concerning the realities of the Republic of Kazakhstan. This research seeks to analyze the challenges and opportunities associated with implementing innovative information security technologies in Kazakhstan across individual, organizational, and national levels. Specifically, this study will investigate how aspects such as infrastructure readiness, investment incentives, and data protection policies influence the successful implementation of cybersecurity technologies, encryption methods, and access control systems for enhancing information security in Kazakhstan.

2. MATERIALS AND METHODS

The methodological approach chosen in this research was a combination of methods of system analysis of the legislation of Kazakhstan in the field of information security and empirical modelling of the key principles of development and implementation of technological innovations in this area. The theoretical basis of this research was the analysis of the results of several scientific studies designed to explore some problematic aspects of the development and implementation of technological innovations to ensure information security and database protection concerning the activities of organisations, citizens, and society in general. The empirical research involved collecting data on the current state of information security in Kazakhstan from scholarly literature, government reports, and technology reviews. Quantitative data was gathered on metrics like cybersecurity incidents, technology adoption rates, and digital infrastructure development. Qualitative data, including expert opinions, legislative analyses, and case studies of information security practices, was also compiled. The empirical modeling methodology utilized this data to map relationships between key variables impacting information security outcomes in Kazakhstan. Threat factors like multi-ethnic tensions and the lack of a domestic electronics industry were modeled against information security goals like data protection and access control. Data on innovative technologies was incorporated to simulate their potential effect on information security.

Application of the method of system analysis of the legislations of the Republic of Kazakhstan in the field of information security and data protection allowed the establishment of the main measures planned by the government of the state in the field of strengthening information security. For the system analysis of legislation, the current laws and regulations related to information security in Kazakhstan were reviewed and analyzed. Specifically, the Cybersecurity Law, the Personal Data Protection Law, and relevant decrees from the past 5 years were examined. The key principles, priorities, and provisions around information protection in these laws were identified and categorized through qualitative coding. Any changes over time in the legislative approach to information security innovations were noted. Some regulations of the current legislation governing the sequence of introduction of technological improvements in the information space of the country, considering the real demands of citizens and society in general for modern technologies capable of ensuring a high level of information security, have been established.

The research also employed purposive sampling to identify threats to information security in Kazakhstan for inclusion in the empirical model. Threats were selected based on their relevance to information security at the individual, organizational, and national levels in the current Kazakhstani context. The specific threats modeled, such as multi-ethnic tensions, the dependence of media on commercial entities, the lack of a domestic electronics industry, and the erosion of cultural values, were chosen due to their significance as reported in recent literature on information security in Kazakhstan. Additionally, examples of information security innovations relevant to Kazakhstan were purposefully selected based on their potential to address current gaps and issues in Kazakhstan's information protection systems. The innovations highlighted, like virtual client protection, enterprise network support, and advanced cloud security, were chosen to demonstrate technologies aligned with Kazakhstan's development programs and information security needs. The use of purposive sampling enabled a focus on legislation, threats, and innovations most salient to understanding information security in the Kazakhstani context based on the research aims. Adding details on the rationale for the selected data sources can help strengthen the methodology.

In addition, the key state interests in the sphere under

consideration were identified, considering the priorities in information protection, interests, and needs of citizens and organisations in the field of information exchange. The main threats to information security at the state level were established, and the components of information security as a state priority were identified. The issues of the interrelation of separate constituent parts of information security, as applied to the activities of organisations and individual private users, were disclosed.

The application of the modelling method allowed the development of a model of the relationship between the main factors that determine the effectiveness of technological innovations in the field of information security. Therewith, a model was developed to prevent threats in this area at the level of organisations and citizens through the use of innovations in the field of information security. It allowed for the identification of both the main factors determining threats in the field of information security and specific opportunities to counteract such threats. During the development of the above-mentioned model, the key areas of development of innovative technologies in the field of information security were identified concerning the realities of the Republic of Kazakhstan.

In addition, a comparative assessment of the effectiveness of specific technological innovations and conventional systems was given. The comparative assessment analyzed key information security technologies like cloud platforms, encryption methods, and access control systems against conventional legacy systems. The criteria used for comparison included: resource efficiency (server capacity utilization, processing power needs); scalability (ability to easily increase capacity); development speed (time required to deploy new features or functionality); responsiveness (ability to rapidly adjust to changes in user needs or threats); innovation (use of new techniques like AI and advanced algorithms). The comparative assessment revealed the advantages of the new technologies, such as improved scalability, faster deployment, and higher responsiveness. This analysis provided evidence for the benefits of emerging information security innovations compared to traditional legacy systems. The main advantages of innovative methods of information protection, which determine the expediency and necessity of their further use, have been highlighted. Specific practical examples of the implementation of innovative technologies in the field of information protection, relevant to date in the context of information security and data protection in the Republic of Kazakhstan are presented.

The chosen combination of methods of this research allowed evaluating the role and significance of technological innovations in the issues of information security in Kazakhstan, considering the needs of government agencies, citizens and organisations. It allowed estimating the prospects for the development of the considered technologies in the future, in the context of the development of the information space of the Republic of Kazakhstan in general.

3. RESULTS

Decree of the President of the Republic of Kazakhstan No. 636 "On approval of the National Development Plan of the Republic of Kazakhstan until 2025 and invalidation of some decrees of the President of the Republic of Kazakhstan" [7], ensured appropriate legislative conditions for the development of the latest technologies and the establishment of prerequisites for the development of demand for innovative technologies according to such priorities as "Technological renewal of industries and digitalisation", and "Establishing the foundations for a new economy". The Leader of the State instructed the Government to prepare several proposals in the following areas:

- Compile a list of Kazakhstani developments in the field of information technologies in the state and quasi-state sectors that can successfully compete with foreign models;
- Significantly simplify the procedures for allocating funds from the state budget of the Republic of Kazakhstan for the development of technological innovations in the field of digitalisation and information security;
- Encourage investment in the development of innovative technologies in the field of information protection and the provision of guarantees to investors in the area of reducing the level of risk of investment operations;
- Develop measures of state control over the targeted use of investments in the sphere of innovative information security technologies.

The effect of innovative technologies as a factor in the information security of the Republic of Kazakhstan is determined by potential threats. Currently, the following threats to information security at the state level are relevant [8]:

(1) The multinationality and multi-confessionalism of Kazakhstan determine increased requirements for information security. It is explained by the fact that the transmission of false information can develop tensions among particular ethnic groups and destabilise the social environment.

(2) The dependence of the mass media on commercial structures results in citizens not receiving the necessary amount of information about aspects of the activities of government bodies that interest them and their intentions. Such information is frequently presented in a distorted form and is not reliable.

(3) The absence of Kazakhstan's electronic industry and the insufficient efficiency of state programs in the field of its development. It may result in the drain of intellectual resources from the country and the impossibility of its participation in the processes of the world division of labour in the sphere of informatisation society.

(4) There are problems ensuring an appropriate level of protection of cultural and moral heritage due to the impossibility of introducing a ban on the dissemination of untruthful information in electronic media. The result may be the erosion of the spiritual and moral base of Kazakhstani society and the expansion of other states in the field of culture.

Information security includes the following components: confidentiality, availability and integrity. Confidentiality in the context of information security implies ensuring that information can be accessed by those who have the necessary authorisation to do this. In the case of access to information posted on Internet resources, these are users who have been authorised. Accessibility of information implies ensuring that authorised users can access it in situations where this is required. Integrity implies ensuring an appropriate level of information reliability and completeness, and the necessary processing capabilities. These components of information security apply exclusively to data protection, while they do not apply to other aspects of this problem, in particular, socio-political ones. The socio-political aspects of information security are considered exclusively as the "world of ideas" and not the "world of data" [4, 9].

In this research, a model of the relationship between the main threats in the field of information security in the context of overcoming them through technological innovations has been developed. This model includes only threats to the information security of users and organisations that are relevant at the moment for the Republic of Kazakhstan. Therewith, innovative means of ensuring the information security of organisations and individual users, used in the development of protection mechanisms, are divided into formal and informal. The former is capable of implementing protective functions without immediate human involvement, while informal means are determined solely by the focus of users' or organisations' actions and establish regulations for this activity. Figure 1 presents a block diagram of the main threats in the sphere of information security in Kazakhstan at the level of enterprises and citizens in the context of the application of innovative information technologies.

The objectives of introducing innovative technologies in the field of information security are to prevent threats and establish the necessary conditions to ensure the protection of the data of organisations and users. The main areas of development of innovative technologies in this area include innovations in the production of information security equipment made of high-quality materials, the development of components of integrated circuits of ultra-high precision, and the introduction of high-tech components in the technical elements of information infrastructure. A distinctive feature of innovative technologies as a factor in information security is their interdependence, which is the reason for their consistent integration. It determines the prospects of their use to solve various technological problems where the application of software of different levels is required. Figure 2 presents the model of interrelationships among the main factors that determine the effectiveness of technological innovations in the field of information security.

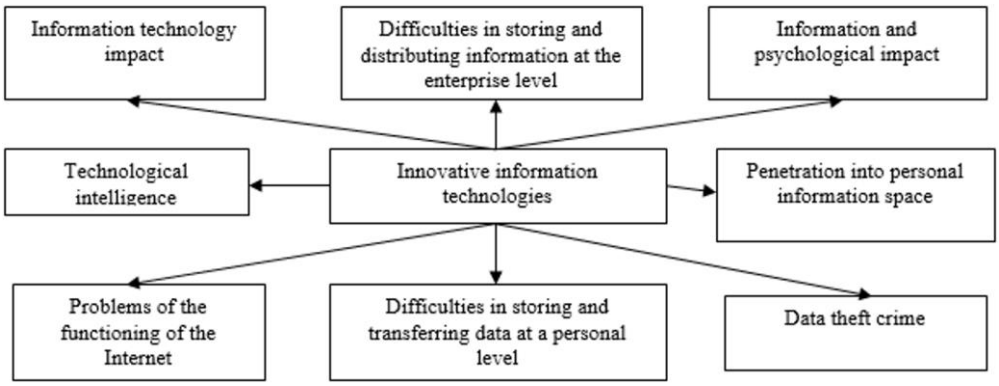

Figure 1. Main threats in the sphere of information security at the level of enterprises and citizens

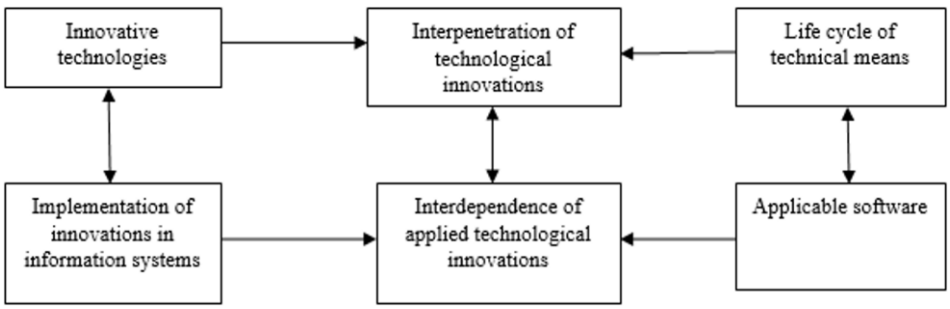

Figure 2. Interrelationship of components determining the effectiveness of technological innovations in the field of information security

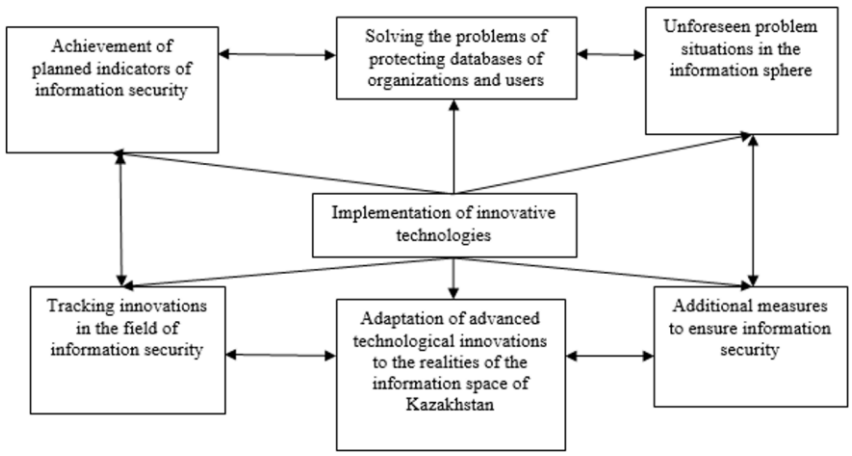

Figure 3. Theoretical model of introduction of innovative technologies in the information space of Kazakhstan (general view)

Software is a key component of information exchange processes. The efficiency of its use determines the life cycle of technical means that perform the functions of accumulation, storage, and transmission of information. Interchangeability and interpenetration of technological innovations determine the possibility of increasing the life cycle of technical means used in the field of data storage. Thus, the effectiveness of the practical application of technological innovations in the field of information storage and transmission security is determined by the volume of their implementation and the quality of interconnection and interchangeability [10]. Figure 3 presents a theoretical model for introducing innovative technologies in the sphere of information space in the Republic of Kazakhstan in the context of information security. Represents a representation of the structural interrelationship of all components.

The presented model represents the structural interrelation of various options for the development of events in the introduction of technological innovations in the information space of the Republic of Kazakhstan. In particular, the introduction of technological innovations in the information space of the country can establish additional, unforeseen situations that require immediate solutions. In addition, the world of information technology is in a state of constant change and development, which necessitates the need to monitor innovations in the field of information protection and their adaptation to the realities of the country. The theoretical probability of the occurrence of various variants of the development of events at the introduction of technological innovations implies the need for advance algorithms for appropriate and timely responses to these changes. From the standpoint of estimating the distribution of options for the development of events, this model takes the form presented in Figure 4.

As follows from the data presented in Figure 4, the introduction of technological innovations is designed to solve the problems of information security for users and individual organisations. If these problems are successfully solved, the planned information security indicators are achieved, expressed in the preservation of specified amounts of data and ensuring secure access to information. In this context, problematic situations in the information space are likely to occur, divided into three main groups: deliberate data theft, accidental information leaks, and violations of the rules of information exchange. In terms of assessing the dynamics of tracking and implementation of technological innovations in the information space of Kazakhstan, the theoretical model takes the form presented in Figure 5.

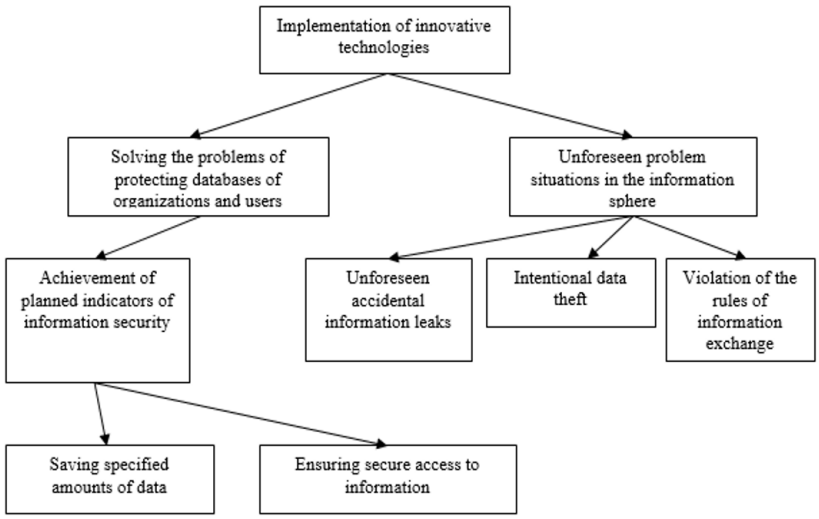

Figure 4. Probabilistic options for the development of events when introducing technological innovations

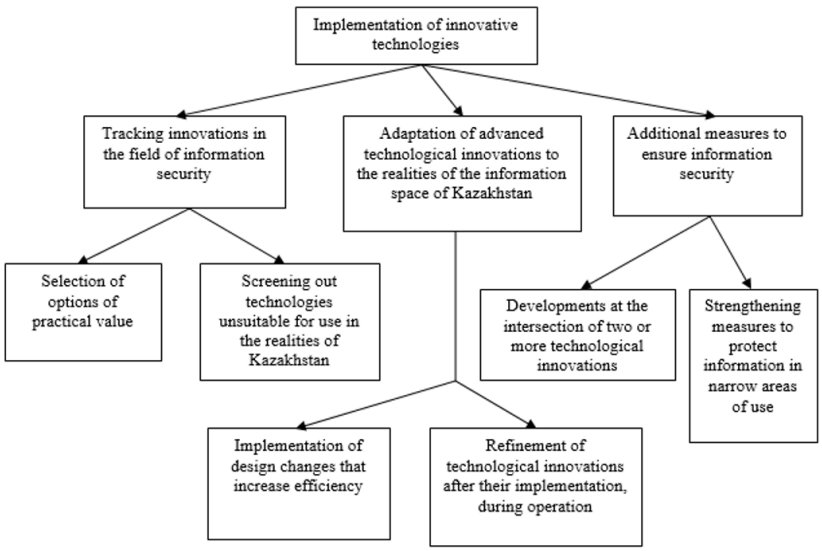

Figure 5. Dynamics of tracking and implementation of innovative technologies in the information space of Kazakhstan

As follows from the data presented in Figure 5, the introduction of technological innovations in the information space of Kazakhstan is associated with the need to develop a set of measures to monitor the effectiveness of their functioning and improve the overall level of technology used in this area. Theoretically, there are three key areas of development possible. Firstly, tracking promising innovations in the field of innovative technologies (including the selection of options that have practical value and eliminating technologies that do not represent value). Secondly, adaptation of technological innovations to the realities of the information space of Kazakhstan (including the introduction of constructive changes in the technologies being prepared for launch, if necessary, and improvement of already functioning innovations). Thirdly, there are some additional measures and several additional measures to improve the quality of the information space in Kazakhstan.

Thus, the theoretical model of the introduction of innovative technologies into the information space of the Republic of Kazakhstan includes various aspects and probabilistic options of events in their systemic interrelation. It concerns both measures to ensure information security and measures to improve the functioning of innovations that have passed the stage of implementation and the monitoring of new, more promising opportunities in this area. While technologies have existed for some time, their application specifically for information security is still emerging and not widely adopted, especially in the Kazakhstani context.

Concerning the realities of the Republic of Kazakhstan, it is advisable to consider at the legislative level the issues of purchasing foreign software to support the Kazakhstani manufacturer [3]. It will contribute to stimulating the production of software of sufficient level in the country for the development of innovations in this area and the establishment of conditions necessary for the implementation of information security programmes. The relevance of this problem is the absence in the country of a sufficient number of scientific personnel in the field of information protection and the weakness of the national school in the field of information security. As a consequence, it is difficult to train specialists capable of competing in this market with graduates of foreign higher education institutions.

Innovative technologies in the context of information security are a natural consequence of investments in the development, testing and implementation of specific technical solutions to update the composition and quality of information security products and improve their functionality. One of them is the introduction of ASIC technology in Kazakhstan, which is based on using integrated specialised microchips. This technology has already been successfully used by several companies operating in the IT sector, as it allows them to gain significant competitive advantages in the field of information security. Back in September 2020, one of the largest data centres with a total capacity of 180 megawatts, based on ASIC technology, was opened in Kazakhstan [11]. Therewith, Google has successfully developed and implemented an integrated highly specialised ASIC processor specifically designed for using artificial intelligence systems based on neural networks.

Nowadays, one of the most effective innovative approaches to managing state information assets and ensuring the necessary level of data protection is the technology of "cloud computing". This technology, adopted in the framework of following the strategy "Kazakhstan-2020", implies using cloud platforms as an opportunity to use the free capacities of cloud servers, which, as a rule, are not used in data centres [12, 13]. This innovative technology allows for increasing the amount of utilised capacity quickly and relatively easily without purchasing expensive server hardware, thus reducing costs significantly. The key advantages of cloud technologies include:

-a significant reduction in the computing power requirements of personal computers, which require only the ability to access the Internet;
-resistance to potential failures;
-ensuring a high level of information security;
-the safety of use in all modes of data processing;
-high speed of processing incoming and outgoing information;
-reduced expenditure on software, support, energy and operating costs;
-saving space on the information carrier.

Table 1 summarises the comparative characteristics of cloud platforms compared to conventional systems, presenting the advantages of using them.

Table 1. Comparison of cloud platforms and conventional systems

Cloud Platforms	Conventional Systems
Application efficiency	
Significant increase in resource efficiency (server capacity utilisation by more than 65-75%)	Insufficient efficiency of resource utilisation (server capacities are usually used at the level of up to 30%)
Ability to aggregate resources and increase system consolidation	Mutual duplication of each other's systems and possibilities for purely fragmented applications
Dramatic productivity gains in application development and management, in the exploitation of network resources, and at the individual private user level	Complexities of systems management
Efficiency	
Receipt according to the service delivery model through proven delivery channels	The need to spend a significant amount of time developing and implementing new servers in specific data centres
The ability to increase and decrease the amount of resources used with virtually no loss of time	The need for significant time expenditures to increase the capacity of the servers in use
Ability to improve responsiveness to changes in user requests	The need for significant time expenditures to increase the capacity of the servers in use
Innovation component	
Ability to shift focus from resource management to server management	The complexities of managing the resources that are available
Innovative solutions in the field of information security and data safety	Inability to apply innovations in the field of information security
Stimulation of entrepreneurial activity	Difficulties in counteracting risk factors

Source: compiled by the author based on Dzhalkibaeva [12]

Innovations in the field of information security, the practical application of which is relevant for Kazakhstan in the context

of the “Digital Kazakhstan” development program adopted at the state level, should include:

(1) Protecting virtual client hardware.

(2) Supports consistency in the deployment of enterprise networks.

(3) Using “big data” to accelerate the detection of cyber-attacks and provide a rapid response to these threats.

(4) Improving container security.

(5) Innovations in cloud storage and processing security.

Protecting virtual client equipment is a separate area of information security that involves using cloud computing and virtualisation technologies. Service providers of this kind provide organisations with a set of network services implemented using specific software. Practical application of this kind of technology will significantly increase productivity and quality of customer service and increase customer coverage, which is extremely important from the standpoint of information security in the Republic of Kazakhstan. Supporting the deployment of corporate networks involves the development of flexible and open cloud-type networks and the partial or complete abandonment of the deployment of fixed networks or high-cost hardware. In general, this contributes to improving the overall level of network security in Kazakhstan. Using “big data” provides a high level of protection for databases and the duration of their storage. Technologies of this kind are based on monitoring events that carry potential threats to information security and suppressing the prospects of their further development.

Improving container security involves using open-source design technologies characterised by ease of deployment and rapid configuration. The application of this technological innovation provides a significant increase in the level of information security and protection of user data. Ensuring the security of cloud storage and processing of data involves increasing the level of security of cloud storage usage. In addition, a high level of data customisation is ensured according to user requests. Innovative technologies as a factor of information security of the Republic of Kazakhstan can ensure a high level of data protection both at the level of the state and individual users. Therewith, they have numerous advantages over conventional information exchange systems, which determines the prospects for their development in the future. Such advantages include: higher responsiveness to changes in the requests of information system users, high-quality accounting and tracking of information, and higher productivity in the operation of information systems.

The results identified key threats to information security in Kazakhstan's specific context, including multi-ethnic tensions, the dependence of media on commercial entities, a lack of domestic electronics industry, and the erosion of cultural values. These threats were modeled to demonstrate their impact on goals like data protection and access control.

4. DISCUSSION

Mandal and Uddin [14], in joint research, examined several problematic aspects in the development and implementation of innovative technologies for information security and database protection. The authors note that among modern developers, there is a rapidly growing interest in the application of technological innovation to develop new architectures, methods, tools, and other intelligent devices that function based on data analysis.

In turn, AlGhamdi et al. [15] examined the general principles of controlling information security provisions in Saudi Arabian government organisations through the introduction of several technological innovations. Researchers pay attention to the fact that investments in the development of innovative database security technologies have increased significantly in several countries, which indicates an understanding of the importance of such problems and the need to address them at the state level. Therewith, the rapidity of technological change and the widespread use of digital operations have necessitated the introduction of innovative technologies as a factor that can fully ensure compliance with the norms of state information security [16, 17]. Drawing on the experience of this work, the threats and solutions for Kazakhstan were specifically modeled based on its particular ethnic, economic, and regulatory context.

For their part, Ali et al. [18] conducted scientific research on information security risks in the example of local government in Australia. The researchers highlight the fact that the adoption of cloud services at the local government level is largely constrained by data security considerations. According to the authors, issues of operational security, data loss awareness and compliance present a set of threats to the government. In turn, this determines the need to develop and implement innovative information security technologies, with control of this process at the government level [19]. An example of the practical application of such technologies is the tendency to run applications in containers instead of virtual machines, allowing through using an open-source platform to support the management of Linux applications within containers [20-22]. The opinion of the researchers fully correlates with the results of this scientific work, as it concerns the issues of establishing a legislative framework to ensure the proper implementation of innovations in the field of information security, and presents practical examples of the application of technological innovations relevant to the information space of modern Kazakhstan. In contrast to this study, the paper empirically analyzed the benefits of innovations such as container security and big data analytics for Kazakhstan. The focus was on alignment with national digitization plans against risk factors.

Therewith, Yang et al. [23], in joint research, considered the general principles of the relationship between science and modern technologies in the field of information security. According to scientists, scientific research is the main driving force of innovation in any technological sphere. Therewith, modern research in the field of personal data protection implies the prospect of establishing a system of interrelations between science and technology that guarantee the high quality of such protection. In addition, it contributes to the increase in the number of patent inventions for innovative technologies in the field of information security [24-27].

Davidson et al. [28] conducted joint scientific research on promising areas of scientific development in the field of data management and the implementation of technological innovations for information security. According to scientists, the application of digital innovations in information security requires fundamentally new technological, scientific and organisational approaches. In this context, the crucial factor is to achieve a high level of information security within an individual organisation or the state in general, which can be achieved through using innovative technological solutions [29, 30]. Building on this, the research involved developing a multivariate model to simulate how threats and technologies

interact in Kazakhstan. This method allowed systematic analysis of implementation factors unique to Kazakhstan.

Vial [31], in research exploring the practical application of digital innovations in data management, highlights the fact that targeted data management is an essential element of data protection. For their part, Yang et al. [32] in scientific research of several problematic aspects of the application of information security risk assessment techniques note that the issues of information security management have gained significant importance since modern companies and organisations have come to rely primarily on their computer networks and systems. Nowadays, maintaining competitiveness is largely related to the ability of enterprises to protect information and reduce the risk of its theft to a possible minimum [33-35]. It is frequently possible only through the use of technological innovations that can provide high-quality protection of enterprise data [36]. According to the authors, such innovations should include using “big data” correlation technologies that allow tracking the probability of “malicious” events.

Therewith, Wang et al. [37] examined the general principles of intrusions and security calculation in cloud data storage based on an improved dynamic algorithm. Researchers note that cloud computing is now widely used for analysing and storing user data as a rather efficient tool. Therewith, according to the authors, the development of innovative systems based on artificial intelligence has contributed to the acceleration of production processes while maintaining a sufficiently high level of protection of users’ data.

Warkentin and Orgeron [38], in joint research, examined information security issues related to using blockchain technology in several public sector applications. The researchers noted that blockchain technology can store a large amount of information, which requires that it be securely protected. According to the researchers, due to the introduction of modern innovative technological solutions in the fields of information security and database protection, government agencies can utilise blockchain technology to provide a wide range of services that go far beyond the distribution of finances. For this purpose, various service data repositories are used for government-user interaction, with services ranging from digital voting to electronic card verification, which are technological innovations for information security and protection of user databases, as applied to using blockchain technologies [39, 40]. The application of modern technological solutions for the protection of information and personal data was considered in the scientific research of Singh et al. [41], designed to explore the general principles of mobile data usage. According to scientists, when making mobile payments, the issues of personal data security should be given special attention, as it is necessary to minimise the probability of loss of user funds. In this context, the development of special digital algorithms for data encryption, which ensure the preservation of their confidentiality, has broad prospects [42, 43].

The findings have important implications for information security practices and policies in Kazakhstan. Identifying the most salient threats guides prioritizing cybersecurity efforts and resource allocation. The results indicate which vulnerabilities and risks need urgent attention in Kazakhstan. The comparative assessment of information security innovations establishes their advantages over status-quo systems. This evidence informs strategic technology investments and upgrading initiatives for enhanced information protection. The findings showcase the benefits of emerging technologies for Kazakhstan's digital infrastructure goals. Additionally, the tailored innovation recommendations create a targeted roadmap for Kazakhstan to boost information security capacities. By focusing on innovations that align with Kazakhstan's landscape, the results guide effective adoption suited to local needs and conditions. This is significant for efficiently bolstering information safeguards.

In the context of an article, a comprehensive approach to studying information security innovation implementation in Kazakhstan involves several future studies. Firstly, conducting comparative studies across multiple developing countries that share similarities with Kazakhstan can provide valuable insights into the generalizable enablers, barriers, and trends in information security innovation adoption across diverse contexts. Secondly, longitudinal studies that track the evolution of threat landscapes and innovation adoption over time within Kazakhstan can offer a dynamic perspective, enhancing foresight and better-informed planning in the field of information security. Thirdly, developing quantitative models tailored to the Kazakhstani context can assist in forecasting the return on investment for various information security innovations, thereby facilitating cost-benefit analysis and prioritization of resources.

5. CONCLUSIONS

This research explored the key factors influencing the successful implementation of innovative technologies for information security in Kazakhstan. The findings revealed that while Kazakhstan's government supports technological innovations through policies like "Digital Kazakhstan," challenges persist due to underdeveloped infrastructure. Threats were found to include multi-ethnic tensions, media reliance on commercial entities, a lack of domestic electronics industry, and the erosion of cultural values. Effective innovations for Kazakhstan could include virtual client protection, enterprise network support, big data analytics, advanced cloud security, and container security. Their benefits over conventional systems were demonstrated through improved efficiency, scalability, accelerated development, responsiveness to threats, and the enabling of new techniques.

The results have significant implications for information security practices and policies in Kazakhstan. The identification of salient threats should guide the prioritization of cybersecurity efforts and resource allocation toward the most vulnerable areas. The evidence on the advantages of emerging innovations makes the case for strategic investments in upgrading Kazakhstan's digital infrastructure and capacities. The innovation recommendations create a tailored roadmap to enhance information security, considering local conditions and needs. The prospects for further research in the field of the development and implementation of innovative technologies as the most important factor in ensuring information security are determined by the rapid pace of the development of science and technology. It determines the development of the information sphere and the growing need for the considered technologies in the context of the need to solve new problems of information security.

REFERENCES

[1] Scientific articles of Kazakhstan. Problems of

introducing innovative technologies in Kazakhstan. https://articlekz.com/article/11264, accessed on Jun. 2, 2023.
[2] Erzhinbek, A., Erkan, T., Berdygulova, A.D., Eleusizova, G.S. (2020). Evolution of innovative development and global the future of education in the era of digitization. East European Scientific Journal, 5(37): 73-76.
[3] Polomarchuk, B. (2021). The problem of ensuring information security of the Republic of Kazakhstan. The Scientific Heritage, 70: 52-55.
[4] Sabitov, D. (2016). Information security Kazakhstan: Data protection and meanings. Institute of World Economics and Politics at the Foundation First President of the Republic of Kazakhstan. https://www.researchgate.net/publication/344726329_Information_Security_in_Kazakhstan_Protection_of_Data_and_Ideas.
[5] Pirounias, S., Mermigas, D., Patsakis, C. (2014). The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. Journal of Information Security and Applications, 19(4-5): 257-271. http://doi.org/10.1016/j.jisa.2014.07.001
[6] Saglam, R.B., Nurse, J.R.C., Hodges, D. (2022). Personal information: Perceptions, types and evolution. Journal of Information Security and Applications, 66: 103163. https://doi.org/10.1016/j.jisa.2022.103163
[7] Decree of the President of the Republic of Kazakhstan No. 636. (2018). On Approval of the National Development Plan of the Republic of Kazakhstan until 2025 and Invalidation of Some Decrees of the President of the Republic of Kazakhstan. https://adilet.zan.kz/rus/docs/U1800000636, accessed on Jun. 02, 2023.
[8] Czvetkó, T., Kummer, A., Ruppert, T., Abonyi, J. (2022). Data-driven business process management-based development of Industry 4.0 solutions. CIRP Journal of Manufacturing Science and Technology, 36(3): 117-132. https://doi.org/10.1016/j.cirpj.2021.12.002
[9] Aebissa, B., Dhillon, G., Meshesha, M. (2023). The direct and indirect effect of organizational justice on employee intention to comply with information security policy: The case of Ethiopian banks. Computers & Security, 130: 103248. https://doi.org/10.1016/j.cose.2023.103248.
[10] Liebenberg, M., Jarke, M. (2023). Information systems engineering with Digital Shadows: Concept and use cases in the Internet of Production. Information Systems, 114: 102182. https://doi.org/10.1016/j.is.2023.102182
[11] (2020). В Казахстане открылся сервисный центр для ASIC-майнеров MicroBT. https://forklog.com/news/v-kazahstane-otkrylsya-servisnyj-tsentr-dlya-asic-majnerov-microbt, accessed on Jun. 02, 2023.
[12] Dzhalkibaeva, A.K. (2021). The role of information and communication technologies in the Republic of Kazakhstan: Current state, problems and ways to improve. In: Materials of the International Scientific and Practical Conference "Modern Trends of Socio-Economic Development of Agro-Industrial Production of Ukraine in the Context of Integration into the World Economy". Nizhyn Agrotechnical Institute, Nizhyn. http://ela.nati.org.ua:8080/bitstream/123456789/534/1/g.alshynbaeva%20rol_informatyz.pdf.
[13] Frank, M., Jaeger, L., Ranft, L.M. (2023). Using contextual factors to predict information security overconfidence: A machine learning approach. Computers & Security, 125: 103046. https://doi.org/10.1016/j.cose.2022.103046
[14] Mandal, N., Uddin, G. (2022). An empirical study of IoT security aspects at sentence-level in developer textual discussions. Information and Software Technology, 150: 106970. https://doi.org/10.1016/j.infsof.2022.106970
[15] AlGhamdi, S., Win, K.T., Vlahu-Gjorgievska, E. (2022). Employees' intentions toward complying with information security controls in Saudi Arabia's public organizations. Government Information Quarterly, 39(4): 101721. https://doi.org/10.1016/j.giq.2022.101721
[16] Fialko, N., Dinzhos, R., Sherenkovskii, J., Meranova, N., Prokopov, V., Babak, V., Korzhyk, V., Izvorska, D., Lazarenko, M., Makhrovskyi, V. (2022). Influence on the thermophysical properties of nanocomposites of the duration of mixing of components in the polymer melt. Eastern-European Journal of Enterprise Technologies, 2(5): 116. https://doi.org/10.15587/1729-4061.2022.255830
[17] Levchenko, V., Pogosov, O., Kravchenko, V. (2023). Cobalt application in repair tools for maintenance and modernisation of NPP equipment. Scientific Herald of Uzhhorod University. Series "Physics", (53): 31-41. https://doi.org/10.54919/physics/53.2023.31
[18] Ali, O., Shrestha, A., Chatfield, A., Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly, 37(1): 101419. https://doi.org/10.1016/j.giq.2019.101419
[19] Kerimkhulle, S., Alimova, Z., Slanbekova, A., Baizakov, N., Azieva, G., & Koishybayeva, M. (2022). The use leontief input-output model to estimate the resource and value added. In 2022 International Conference on Smart Information Systems and Technologies (SIST), Nur-Sultan, Kazakhstan, pp. 1-5. https://doi.org/10.1109/SIST54437.2022.9945746
[20] Kerimkhulle, S., Kerimkulov, Z., Aitkozha, Z., Saliyeva, A., Taberkhan, R., Adalbek, A. (2022). The estimate one-two-sided confidence intervals for mean of spectral reflectance of the vegetation. Journal of Physics: Conference Series, 2388(1): 012160. https://doi.org/10.1088/1742-6596/2388/1/012160
[21] Yasin, U., Madina, K., Olga, K. (2020). Improved technology for new-generation Kazakh national meat products. Foods and Raw materials, 8(1): 76-83. https://doi.org/10.21603/2308-4057-2020-1-76-83
[22] Kalinichenko, A., Havrysh, V. (2019). Feasibility study of biogas project development: Technology maturity, feedstock, and utilization pathway. Archives of Environmental Protection, 45(1): 68-83. https://doi.org/10.24425/aep.2019.126423
[23] Yang, Y.P.O., Shief, H.M., Tzeng, G.H. (2013). A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. Information Sciences, 232: 482-500. https://doi.org/10.1016/j.ins.2011.09.012
[24] Madiyarova, A., Ziyadin, S., Blembayeva, A., Doszhan, R. (2018). Modern trends in digitalization of tourism industry. In Proceedings of the 32nd International Business Information Management Association Conference, IBIMA 2018-Vision 2020: Sustainable Economic Development and Application of Innovation

Management from Regional expansion to Global Growth, pp. 7990-7997.
[25] Mustafin, A., Kantarbayeva, A. (2022). A model for competition of technologies for limiting resources. Vestnik Yuzhno-Ural'skogo Universiteta. Seriya Matematicheskoe Modelirovanie i Programmirovanie, 15(2): 27-42. https://doi.org/10.14529/mmp220203
[26] Fialko, N., Dinzhos, R., Sherenkovskii, J., Meranova, N., Aloshko, S., Izvorska, D., Korzhyk, V., Lazarenko, M., Mankus, I., Nedbaievska, L. (2021). Establishment of regularities of influence on the specific heat capacity and thermal diffusivity of polymer nanocomposites of a complex of defining parameters. Eastern-European Journal of Enterprise Technologies, 6(12): 114. https://doi.org/10.15587/1729-4061.2021.245274
[27] Fialko, N., Dinzhos, R., Sherenkovskii, J., Meranova, N., Navrodska, R., Izvorska, D., Korzhyk, V., Lazarenko, M., Koseva, N. (2021). Establishing patterns in the effect of temperature regime when manufacturing nanocomposites on their heat-conducting properties. Eastern-European Journal of Enterprise Technologies, 4(5): 112. https://doi.org/10.15587/1729-4061.2021.236915
[28] Davidson, E., Wessel, L., Winter, J.S., Winter, S. (2023). Future directions for scholarship on data governance, digital innovation, and grand challenges. Information and Organization, 33(1): 100454. https://doi.org/10.1016/j.infoandorg.2023.100454
[29] Kurmanov, A.K., Ermaganbet, A.C., Ahanov, S.M., Rahatov, S.Z., Ryspayev, K.S., Ryspayeva, M.K. (2014). Classification of vibrators. Life Science Journal, 11(S7): 410-412.
[30] Shaimurunov, S., Ryspayev, K., Ismailov, A., Zhikeyev, A., Salykov, B. (2023). Study of the Efficiency of Using Facilities Based on Renewable Energy Sources for Charging Electric Vehicles in Kazakhstan. International Journal of Sustainable Development & Planning, 18(4): 1263-1269. https://doi.org/10.18280/ijsdp180431
[31] Vial, G. (2023). Data governance and digital innovation: A translational account of practitioner issues for IS research. Information and Organization, 33(1): 100450. https://doi.org/10.1016/j.infoandorg.2023.100450
[32] Yang, X., Feng, L., Yuan, J. (2023). Research on linkage of science and technology in the library and information science field. Data and Information Management, 7(2): 100033. https://doi.org/10.1016/j.dim.2023.100033
[33] Hasanli, R., Aliyev, I., Poladov, N., Azimova, L., Tagiyev T. (2022). Isothermal transformations in high-strength cast iron. Scientific Herald of Uzhhorod University. Series "Physics", (51): 48-58. https://doi.org/10.54919/2415-8038.2022.51.48-58
[34] Shevko, V., Afimin, Y., Karataeva, G., Badikova, A., Ibrayev, T. (2021). Theory and technology of manufacturing a ferroalloy from carbon ferrochrome dusts. Acta Metallurgica Slovaca, 27(1): 23-37. https://doi.org/10.36547/ams.27.1.745
[35] Smailova, G., Yussupova, S., Uderbaeva, A., Kurmangaliyeva, L., Balbayev, G., Zhauyt, A. (2018). Calculation and construction of the tolling roller table. Vibroengineering Procedia, 18: 14-19. https://doi.org/10.21595/vp.2018.19908
[36] Mazakov, T., Jomartova, S., Ziyatbekova, G., Aliaskar, M. (2020). Automated system for monitoring the threat of waterworks breakout. Journal of Theoretical and Applied Information Technology, 98(15): 3176-3189
[37] Wang, W., Ren, L., Chen, L., Ding, Y. (2019). Intrusion detection and security calculation in industrial cloud storage based on an improved dynamic immune algorithm. Information Sciences, 501: 543-557. https://doi.org/10.1016/j.ins.2018.06.072
[38] Warkentin, M., Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. International Journal of Information Management, 52: 102090. https://doi.org/10.1016/j.ijinfomgt.2020.102090
[39] Abudaqa, A., Hilmi, M.F., Almujaini, H., Alzahmi, R.A., Ahmed, G. (2021). Students' perception of e-Learning during the Covid Pandemic: A fresh evidence from United Arab Emirates (UAE). Journal of E-Learning and Knowledge Society, 17(3): 110-118. https://doi.org/10.20368/1971-8829/1135556
[40] Tserklevych, V., Prokopenko, O., Goncharova, O., Horbenko, I., Fedorenko, O., Romanyuk, Y. (2021). Virtual Museum Space as the Innovative Tool for the Student Research Practice. International Journal of Emerging Technologies in Learning, 16(4): 213-231. https://doi.org/10.3991/ijet.v16i14.22975
[41] Singh, N., Sinha, N., Liebana-Cabanillas, F.J. (2020). Determining factors in the adoption and recommendation of mobile wallet services in India: Analysis of the effect of innovativeness, stress to use and social influence. International Journal of Information Management, 50: 191-205. https://doi.org/10.1016/j.ijinfomgt.2019.05.022
[42] Tanchak, A., Katovsky, K., Haysak, I., Adam, J., Holomb, R. (2022). Research of spallation reaction on plutonium target irradiated by protons with energy of 660 MeV. Scientific Herald of Uzhhorod University. Series "Physics", 52: 36-45. https://doi.org/10.54919/2415-8038.2022.52.36-45
[43] Aliaskar, M., Mazakov, T., Mazakova, A., Jomartova, S., Shormanov, T. (2022). Human voice identification based on the detection of fundamental harmonics. In 2022 IEEE 7th International Energy Conference (ENERGYCON), Riga, Latvia, pp. 1-4. https://doi.org/10.1109/ENERGYCON53164.2022.9830471