Information Security in the Context of Global Society: Essence and Development Trends

Submitted: 29 July 2025
Reviewed: 13 October 2025
Revised: 4 November 2025
Accepted: 5 November 2025

Aigerim Ibrayeva[*]
https://orcid.org/0000-0002-1341-753X
Saniya Sarsenova[**]
https://orcid.org/0000-0003-3134-284X
Kairat Abdrakhmanov[***]
https://orcid.org/0009-0009-7873-5457
Maira Dyussembekova[****]
https://orcid.org/0000-0002-0604-1642
Karlygash Kondykerova[*****]
https://orcid.org/0009-0009-4415-2915

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v18i2.59112

Abstract

[Purpose] The purpose of this study was to identify the key aspects of ensuring information security in the Republic of Kazakhstan and to analyse international approaches to this issue.
[Methodology/approach/design] The research methodology included content analysis of regulatory legal acts governing information security policies, an examination of international cybersecurity practices (USA, China, Germany, France). As part of the study, a survey was conducted in Kazakhstan. The study involved 103 respondents aged 21 to 55, including 57 men and 46 women. The survey was conducted from January to March 2025 via the Google Forms online platform, and a comparative analysis of the readiness and security levels of information systems in different countries was carried out.
[Findings] The main findings of the study were as follows: Kazakhstan has a strategically important programme for digital transformation and cybersecurity development. However, survey data indicate that 56% of respondents highlight a shortage of qualified cybersecurity professionals. Only 45% of respondents consider existing educational programmes for training such specialists to be effective. Meanwhile, 74% of respondents note significant

[*]Dean of the Higher School of Social Sciences and Humanities, Astana International University, Astana, Republic of Kazakhstan. Email: aige.ibrayeva@gmail.com
[**]PhD, Associate Professor at the Higher School of Law, Astana International University, Astana, Republic of Kazakhstan. Email: s_sarsenova@outlook.com
[***]Researcher at the International Cooperation and Student Affairs, Astana International University, Astana, Republic of Kazakhstan. Email: abdrakhmanov.k34@outlook.com
[****]Researcher at the Department of Political Science, L.N. Gumilyov Eurasian National University, Astana, Republic of Kazakhstan. Email: maira_dyus@hotmail.com
[*****]Researcher at the Higher School of Social Sciences and Humanities, Astana International University, Astana, Republic of Kazakhstan. Email: k.kondykerova@hotmail.com

gaps in digital literacy among the population, which poses a major threat to national security. The obtained results allow for an assessment of the current state of cybersecurity in Kazakhstan and identify key issues requiring immediate resolution, particularly the insufficient level of workforce training and the absence of an effective cyber threat monitoring system. This enables government authorities and businesses to draw conclusions for improving state cybersecurity policies. The study culminates in the development of recommendations for enhancing information security policies in Kazakhstan. Specifically, the need to improve cybersecurity education programmes, increase funding for cyber defence infrastructure development, and establish rapid response mechanisms to cyberattacks has been identified.

[Practical implications] The research findings can be utilised by government agencies, educational institutions, and enterprises to develop strategies for combating cybercrime and enhancing national security in the context of digitalisation.

[Originality/value] The paper provides a comprehensive analysis of Kazakhstan's cybersecurity landscape, identifying key challenges like workforce shortages and digital literacy gaps, and offers actionable recommendations for policymakers, educators, and businesses to enhance national information security.

Keywords: Cyber Threats. Digital Literacy. Data Protection. Legislative Regulation. Challenges and Threats.

INTRODUCTION

In a global society where information flows are rapidly expanding, the issue of information security is becoming increasingly critical. The intensive integration of digital technologies into all spheres of life – from the economy to education – is accompanied by growing risks associated with data breaches, cyberattacks, and information manipulation. These challenges necessitate a systemic analysis of the essence of information security as a multifaceted phenomenon encompassing technical, legal, ethical, and social dimensions. Given the increasing dependence of states, businesses, and citizens on information systems, there is a heightened need for effective mechanisms to safeguard the digital space. Simultaneously, new trends are emerging in this field: the growing role of artificial intelligence in cyber defence, enhanced international cooperation in information security, and the adaptation of legislation to new challenges. Research into these trends is highly relevant in the context of ensuring stability, trust in the information environment, and the preservation of national sovereignty in an era of global interdependence.

A significant number of researchers have explored this topic, offering diverse perspectives. For instance, according to a study by Azanbay (2024), innovative technologies have played a pivotal role in shaping the information security system of the Republic of Kazakhstan. The author emphasised the

importance of implementing IT solutions as a safeguard against external and internal threats in the digital environment. The work analysed specific examples of technology application in information risk management, noting that the development of national IT infrastructure has been fundamental in ensuring stability amid global digital pressures. Myrzakhmetov et al. (2020) highlighted the significance of a regulatory framework in fostering an information culture among youth as a critical security factor. Their study demonstrated that systematic cultivation of critical thinking towards information was key to resilience against manipulation and destructive content. The authors examined Kazakhstan's legislative initiatives aimed at enhancing information literacy, stressing the role of educational institutions as primary agents in developing digital competencies among learners.

Kozhan et al. (2025) proposed a philosophical and cultural studies approach to analysing digitalisation as a civilisational phenomenon, exploring its impact on societal values. The authors argued that digital transformation brings not only technological opportunities but also risks related to privacy erosion and the weakening of ethical norms. The article addressed the need to harmonise technological progress with the preservation of humanistic principles, with particular attention paid to the influence of digital culture on younger generations and the transformation of social relations. The work of Duisenbekuly et al. (2024), dedicated to food security, contained important conclusions regarding the necessity of integrating security strategies into various spheres of state policy, including information security. The authors analysed complex threats arising from changes in the global environment that affect state security, underscoring the importance of interstate cooperation in developing crisis response mechanisms. The experience of Kazakhstan and Azerbaijan was examined as an example of a strategic approach to national security development.

The development of an innovative ecosystem in the Republic of Kazakhstan was examined by Nauryzbaeva et al. (2024). The authors emphasised the importance of integrating innovations into various sectors of the economy to ensure the country's competitiveness at the global level. The study noted that the development of scientific and technological potential is a crucial factor in achieving stable economic growth in the context of digitalisation. It also addressed the main challenges and barriers to the effective implementation of innovation strategies in Kazakhstan. Nussipova et al. (2023) explored issues related to the security of the information environment in Kazakhstan amid the pandemic, fake news, and global information threats. The authors highlighted the need to improve the state's information policy to protect against manipulation and disinformation. The study analysed instances of information attacks that occurred during the pandemic and their impact on the country's social stability. It was noted

that enhancing the level of information security requires the development of national programmes to combat fake news.

Key trends in the formation of the internet space and information society in Kazakhstan were examined by Oralova (2022). The author underscored the importance of developing digital infrastructure to ensure equal access to information in the context of globalisation. The study provided a detailed analysis of challenges in regulating the online environment, as well as issues related to maintaining information security in virtual spaces. It was noted that the Kazakhstani government should continue to refine legislation to protect user data and counter cyber threats. Seidakhmetova et al. (2023) investigated the training of specialists in the field of information security. The authors stressed the necessity of upskilling professionals in this domain to safeguard digital resources. The article examined training methodologies, specialist education programmes, and the role of universities in developing competent personnel. It was noted that the evolving technological landscape necessitates continuous adaptation of educational standards to meet new security requirements. Zabikh (2020) analysed international practices in the legal provision of information security and their potential application in the Republic of Kazakhstan. The author highlighted the need to harmonise national legislation with international standards to ensure effective protection of information resources. The study reviewed examples from international practice where successful strategies to counter cyber threats had been implemented and proposed ways to adapt these experiences to the Kazakhstani context. Zhaparalina et al. (2024) studied the impact of information cooperation in Central Asia on Kazakhstan's interests and foreign policy. The authors argued that, in the context of globalisation, collaboration among Central Asian states in the field of information security holds strategic significance. The article examined mechanisms of international cooperation to counter information threats and ensure regional stability. It was noted that proactive information diplomacy is a key element in shaping Kazakhstan's foreign policy strategy.

Despite considerable academic interest in information security, existing research has insufficiently addressed issues such as cross-sectoral coordination of security policies, long-term forecasting of digital risks, and the socio-cultural impact of digitalisation on the formation of information culture in Kazakhstan.

The study aimed to identify the key features of state policy in the field of information security in the Republic of Kazakhstan amid digital transformation and growing global cyber threats. The research objectives included: analysing the regulatory framework and key documents governing information security in Kazakhstan; conducting a comparative analysis of international cybersecurity practices to identify relevant models; and determining major challenges, trends,

and formulating practical recommendations for improving information security policies.

MATERIALS AND METHODS

The study was conducted between January and March 2025. In this study, the "civilisational approach" was applied to understand how digital transformation and cybersecurity intersect with national identity and values, particularly in Kazakhstan's context. This approach highlights the cultural and social dimensions of information security, emphasizing the need for local digital environments that reflect Kazakhstani societal norms. Meanwhile, the "systems approach" was employed to analyze information security as a complex, interconnected issue within the broader national security framework. By examining the regulatory, technological, and human factors that contribute to security risks, this approach provided a comprehensive understanding of the systemic challenges Kazakhstan faces in protecting its information infrastructure. The theoretical foundations of the study were based on the works of scholars such as Cavelty and Wenger (2020), González-Granadillo et al. (2021), and Zabikh (2020). These researchers were selected due to their contributions to the development of concepts related to the information society and the transformation of the global environment under the influence of information technologies.

A content analysis was conducted on regulatory documents governing information security policies. Primary focus was given to of the Republic of Kazakhstan No. 269 “On Approval of the Concept of Digital Transformation, Development of the Information and Communication Technology Industry and Cybersecurity for 2023-2029” (2023). Additionally, the experiences of the United States (NATIONAL CYBERSECURITY STRATEGY, 2023), the People’s Republic of China (ORDER OF THE PRESIDENT…, 2021), and the European Union (EUROPEAN COMMISSION, 2025) were analysed to identify current international trends in building an effective information security system. These documents and countries were selected for analysis due to their significant contributions to the development and implementation of digital transformation and information security strategies, which are relevant for studying global trends and best practices in the respective fields. A comparative analysis of approaches to information security in Kazakhstan, the US, China, and the European Union was also conducted. A SWOT analysis was performed to identify key strengths and weaknesses, as well as external and internal threats to the information security of the Republic of Kazakhstan.

Within the framework of the study, a questionnaire survey was conducted in Kazakhstan. The study involved 103 respondents aged 21 to 55, including 57 men and 46 women. The survey was carried out from January to March 2025 via

the Google Forms online platform. Participants included IT professionals (25 individuals), students in technical fields (30 individuals), employees in education and public sector (25 individuals), as well as digital transformation experts (23 individuals). Since the survey included multiple-choice questions allowing for percentage-based responses (e.g., selecting the most dangerous threat sources or the use of specific security tools), percentage values were used for evaluation, enabling the identification of response frequencies for each category. The survey results were analysed using the independent samples t-test to analyze the differences in perceptions of information security and digital transformation among the various respondent groups based on their professional backgrounds. This approach allowed for an assessment of the influence of professional background and experience on respondents' perceptions of information security and digital transformation in Kazakhstan. Respondents were presented with 15 original questions, including:

1. How would you assess the overall level of information security in Kazakhstan?
2. Which threat sources do you consider most dangerous: internal or external?
3. To what extent do you trust government agencies in the field of cybersecurity?
4. Have you personally encountered cases of fraud or cyberattacks?
5. Do you believe the level of personal data protection is sufficient?
6. How important, in your opinion, is cyber hygiene in daily life?
7. Which digital security tools do you use (antivirus, VPN, 2FA)?
8. How crucial is international cooperation in cybersecurity for Kazakhstan?
9. Is legislative regulation of social media content necessary?
10. Which technologies do you consider most risky for information security?
11. Have you received specialised training in information security?
12. How crucial is international cooperation in cybersecurity for Kazakhstan?
13. What, in your opinion, are the main risks to the country's information sovereignty?
14. Does the state invest sufficient resources in the development of cyber defence?
15. What priority measures do you consider necessary to strengthen information security?

The study adhered to the provisions of the Code of Ethics of the American Sociological Association. To forecast future developments in information

security, scenario analysis was applied, within which three probable scenarios were developed: optimistic (institutional strengthening, international cooperation, digital literacy), pessimistic (increased external interference, cyberattacks, political manipulation), and inertial (persistence of current risks without significant changes). This allowed for the delineation of potential trajectories in security policy development amid growing global digital interdependence. Recommendations were formulated for improving the information security system of the Republic of Kazakhstan.

RESULTS

Regulatory and legal foundations of information security policy in the Republic of Kazakhstan

The globalisation of information processes has become a defining characteristic of modern civilisation. Digital technologies have radically transformed social, political, economic, and security structures, shaping a new reality – the information society. In this system, information has evolved into a strategic resource, simultaneously serving as a tool for development, a means of influence, and a source of potential threats. Amid geopolitical instability and the rise of hybrid conflicts, the issue of information security has gained particular relevance – as a guarantee of state stability, sovereignty preservation, and societal protection from destructive informational influence. In the digital environment, information security is no longer limited to technical or military defence. It is a multidimensional phenomenon encompassing cultural, legal, psychological, and social aspects. Technologies have acquired the capacity to influence society, transform political processes, shape or destabilise public opinion, and pose risks to critical infrastructure.

The Republic of Kazakhstan is among the countries actively integrating digital technologies into all spheres of life. Resolution of the Government of the Republic of Kazakhstan No. 269 (2023) was adopted, which outlined priorities for creating a secure digital environment. These include the development of cyber defence infrastructure, enhancing public digital literacy, and formulating a national strategy for resilience against information threats. The urgency of these measures is corroborated by statistics: in 2023 alone, Kazakhstan recorded over 13,000 unauthorised access attempts to state information systems. There has been increased activity in bot networks and the dissemination of fake news aimed at destabilising the socio-political situation. This underscores the transformation of information into a tool for coercion, manipulation, and interference in state affairs. Key institutions of information security operate in the country: the Committee of

Information Security of the Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan (2024), the KZ-CERT (2024), and the State Technical Service (2025). Additionally, the National Cyber Threat Management System has been established (COMMITTEE OF INFORMATION SECURITY…, 2024), incorporating centralised monitoring, incident response, and interagency coordination. However, despite positive developments, systemic challenges persist: low levels of digital literacy among the population, reliance on foreign software, legislative gaps, and heightened vulnerability of youth to manipulative content on social media. This highlights the need for fostering information-cultural security, which entails supporting national informational content, developing critical thinking, and enhancing media literacy. An information-security culture reflects an organization's ongoing commitment to keeping its information safe.

In this context, the civilisational approach is of particular importance, as it enables the analysis of not only technological but also cultural transformations within the information space. The proliferation of global digital platforms based on Western behavioural models influences the identity of Kazakhstani youth, displacing national values (LI et al., 2024; URUMKULOVA, 2022). In this regard, the state must develop its own digital environments that reflect local cultural and moral frameworks. Simultaneously, Kazakhstan is integrating into the global information space by enhancing its cybersecurity infrastructure and information risk management. The concept of the information society, which underpins the national digital policy, highlights the necessity of harmonising technological progress with security. Without adequate protection of information flows, the country may face not only economic losses but also a loss of control over its socio-cultural space (ZHETPISBAYEV et al., 2017; ZHANZHUMENOV et al., 2022). Thus, information security in Kazakhstan is regarded as a multifaceted issue encompassing digital transformation, national interests, resilience to external and internal influences, and the need to establish a new model of cultural sovereignty in the digital era. To better understand what Kazakhstan can learn from other countries' experiences, a comparative analysis was conducted, presented in Table 1.

Country/Region	Priorities	Implementation Features
Kazakhstan	Development of information and communication technologies (ICT), digitalisation of public administration; protection	Institutional reforms in cybersecurity; Involvement of state security agencies; Focus on national security

	of critical infrastructure; enhancement of national cybersecurity	
USA	Collective cyber defence; building resilience against cyberattacks; public-private cooperation	Active engagement of the private sector in cybersecurity; multi-level cyber defence; global alliances to combat cybercrime
China	National data control; cyber sovereignty; countering external interference	Centralised cyber governance; Strict regulation of foreign companies; restrictions on western technologies
EU (Germany, France)	Protection of critical infrastructure; common EU-wide regulations; strengthening European cyber resilience	Joint European cybersecurity initiatives; development of a unified European cybersecurity market; coordinated response to global threats

Table 1 – Comparative analysis of information security approaches

The comparative analysis of information security approaches in Kazakhstan, the USA, China, Germany, and France demonstrates that each country has its own strategy and priorities, reflecting national needs and global challenges. However, despite strong strategic initiatives, Kazakhstan should consider certain aspects of other countries' experiences to further strengthen its cybersecurity system. Kazakhstan should significantly enhance cooperation with the private sector. The USA actively develops public-private partnerships in cybersecurity, ensuring not only more effective protection but also fostering innovative solutions through joint efforts between the state and private companies. Additionally, attention should be paid to the development of cyber defence infrastructure, a key element of the US strategy. The private sector, closely collaborating with the government, enables swift and effective responses to cyberattacks. China exemplifies strict regulation and national control over cyberspace and data. As Kazakhstan also faces challenges related to cyber sovereignty and safeguarding national interests, its approach could be reinforced by clearer mechanisms for monitoring foreign technologies and companies operating in the country. In particular, it is crucial to strengthen national control over critical infrastructure and data to minimise external threats. Regarding the

European Union, its cybersecurity approach is based on unified principles adhered to by all member states. The EU's legal framework and intergovernmental cooperation are among the most advanced globally.

Challenges and threats to information security: international and national contexts

Kazakhstan could draw upon European experience in integrating various levels of policy and establishing a unified legal framework for cybersecurity. When referring to "integrating various levels of policy," the focus is on coordinating policies across different tiers of government, such as local, regional, and national levels, to ensure cohesive and unified action. The EU's expertise in data protection and personal privacy is also particularly relevant in the context of rapidly evolving digital technologies. Overall, it would be prudent for Kazakhstan to combine the experience of other countries with its own national specificities. Enhanced cooperation with international partners, the adoption of cutting-edge technologies and regulatory frameworks, and more active engagement of the private sector will enable the country to strengthen its cybersecurity and adapt to the fast-changing global digital environment. To identify key threats, advantages, and significant vulnerabilities, an information security analysis was conducted, as presented in Table 2.

Strengths	**Weaknesses**
Existence of a National Cyber Threat Management System	Insufficient public awareness of digital security fundamentals
Development of digital technologies and cyber defence infrastructure	Dependence on foreign software
Establishment of an effective cybersecurity policy (Digital Transformation Concept)	Lagging legislative framework for cybersecurity
Opportunities	Threats
Information expansion	Presence of comprador businesses (locally owned firms or individuals that act as intermediaries between foreign businesses and the local economy)
Manipulation of public consciousness through social platforms and cyberattacks	Political dependence of information resources

Information-psychological influence via technological tools (disinformation, fake campaigns, bot networks)	Use of criminal kompromat as a tool of coercion
Opportunities	**Threats**
Information Expansion (The rise of digital information creates opportunities for more efficient government services, e-commerce, and citizen engagement through the digital transformation agenda)	Presence of Comprador Businesses. These intermediaries may enable foreign influence over Kazakhstan's digital infrastructure and resources, presenting potential risks to national sovereignty and information security.
Manipulation of Public Consciousness Through Social Platforms and Cyberattacks. (By leveraging social media for public communication and defense, Kazakhstan can counteract misinformation, reduce vulnerability to disinformation campaigns, and promote cybersecurity awareness.)	Political control over information can lead to censorship or manipulation of public opinion, weakening the transparency and reliability of digital media.
	The weaponization of sensitive personal or political information to influence individuals or government decisions poses a significant risk to Kazakhstan's political and social stability.

Table 2 – SWOT analysis of information security in the Republic of Kazakhstan

The conducted SWOT analysis demonstrates that the information security of the Republic of Kazakhstan possesses both significant advantages and notable weaknesses that require attention to further strengthen national security. Internal threats, such as the political dependence of information resources and the use of criminal kompromat, as well as external challenges, including cyberattacks and information expansion, necessitate a comprehensive approach to reinforcing information security (APAKHAYEV et al., 2018; MEHLA & MEHLA, 2024). Considering global trends, Kazakhstan must develop strategies that integrate advanced technologies into cyber defence while simultaneously raising public awareness of risks and the importance of data protection in the digital age.

In Kazakhstan, a range of digital tools and programmes are employed to ensure effective information security, helping to counter diverse cyber threats and safeguard data at both governmental and private sector levels (IASECHKO et al., 2020; ALLAHVERDIYEV, 2023). One of the primary tools is antivirus software, which protects computer systems from viruses, malware, and cyber threats. Software from companies such as Kaspersky, ESET NOD32, and Bitdefender is widely used to scan systems for malicious programmes, block attacks, and secure personal data. These antiviruses detect and neutralise viruses, trojans, and other types of malicious software, which are among the key threats in the digital environment. To enhance personal account security and prevent unauthorised access, two-factor authentication (2FA) systems are actively utilised. This technology provides an additional layer of protection for online accounts by requiring not only a password but also a secondary verification code sent to a mobile device or generated via dedicated applications. The use of 2FA helps mitigate attacks even if a malicious actor obtains a user's password. Another critical tool is virtual private networks (VPNs), which ensure online anonymity, protect data during transmission, and prevent user activity tracking. By encrypting traffic, VPNs allow users to bypass content restrictions and reduce the risk of data interception by malicious actors – particularly important when using public Wi-Fi networks. To defend against phishing and other forms of fraud, many users also employ firewalls and intrusion detection/prevention systems (IDS/IPS). These tools monitor suspicious activities and block malicious attempts to access computer networks and servers. These instruments represent only part of Kazakhstan's broader information security strategy, yet their use is critical in ensuring adequate data protection and countering cyberattacks. They assist not only private users but also businesses and government institutions in actively resisting growing digital threats. To assess awareness, attitudes, and perceptions of contemporary information threats among the public and professionals, a survey was conducted, with results presented in Table 3.

Question	Responses	Percentages
1. How would you assess the overall level of information security in Kazakhstan?	High	12%
	Medium	56%
	Low	32%
2. Which threat sources do you consider most dangerous: internal or external?	Internal	43%
	External	57%
3. To what extent do you trust government bodies in cybersecurity?	Fully trust	18%
	Somewhat trust	39%
	Do not trust	43%

4. Have you personally encountered fraud or cyberattacks?	Yes	37%
	No	63%
5. Do you believe the level of personal data protection is sufficient?	Yes	24%
	No	76%
6. How important is cyber hygiene in daily life, in your opinion?	Very important	78%
	Moderately important	16%
	Slightly important	6%
7. Which digital security tools do you use (antivirus, VPN, 2FA, others)?	Antivirus	45%
	VPN	34%
	2FA	21%
8. How effectively is disinformation countered in Kazakhstan, in your view?	Very effective	12%
	Moderately effective	48%
	Ineffective	40%
9. Is legislative regulation of social media content necessary?	Yes	82%
	No	18%
10. Which technologies do you consider most risky for information security?	Artificial intelligence	29%
	Internet of Things (IoT)	43%
	5G technologies	28%
11. Have you received specialised training in information security?	Yes	20%
	No	80%
12. How important is international cooperation in cybersecurity for Kazakhstan?	Very effective	63%
	Moderately effective	27%
	Not important	10%
13. What, in your opinion, are the main risks to the country's information sovereignty?	Information expansion	55%
	Cyberattacks	30%
	Dependence on foreign technologies	15%
14. Does the state invest sufficient resources in cyber defence development?	Yes	23%
	No	77%

15. What priority measures do you consider necessary to enhance information security?	Raising public awareness	49%
	Developing national cyber defence technologies	36%
	Establishing an effective legal framework	15%

Table 3 – Survey results on information security in Kazakhstan

The survey results indicate that 56% of respondents assess the level of information security in Kazakhstan as average, while 32% consider it low, highlighting significant challenges in this domain. A majority (57%) perceive external threats as more dangerous, whereas 43% regard internal threats as more critical. Regarding trust in governmental cybersecurity institutions, only 18% of respondents report "high trust", while 43% express distrust. Concurrently, 37% of respondents have experienced fraud or cyberattacks. Most (76%) consider the level of personal data protection insufficient. Meanwhile, 78% emphasise the importance of cyber hygiene in daily life. Concerning the use of digital security tools, 45% of respondents employ antivirus software, 34% use VPNs, and 21% rely on 2FA. Regarding the effectiveness of countering disinformation, 48% believe this issue is addressed with moderate efficiency. Legislative regulation of social media content is supported by 82% of respondents, while 63% consider international cybersecurity cooperation highly important for Kazakhstan. As for the primary risks to information sovereignty, 55% associate them with information expansion. Additionally, 77% point to insufficient state investment in cybersecurity development.

Cybercrime poses a serious challenge to the Republic of Kazakhstan, negatively impacting the economy and national stability. With the advancement of digital technologies, a rise in cybercrime has been observed, necessitating a comprehensive approach to address this issue. In 2023, Kazakhstan recorded over 223 million cyberattack attempts by foreign hackers. The highest number of attacks targeted local executive bodies – approximately 133.5 million attempts (OMIRGAZY, 2024). The main types of cybercrime include online fraud – an increasing number of deception cases conducted via the Internet, resulting in substantial financial losses among citizens; attacks on financial institutions – attempts to steal financial assets or compromise banking systems; and attacks on government agencies – efforts to gain unauthorised access to state databases or systems for the purposes of intelligence gathering or sabotage. In response to

escalating cyber threats, the Ministry of Internal Affairs of Kazakhstan has established a new department dedicated to combating cybercrime. This unit focuses on tackling online fraud, blocking fraudulent calls, and protecting citizens from cybercriminal activities. As a result of the measures taken, over 43 million fraudulent calls have been blocked, and citizens have recovered more than 2 billion tenge that could have been transferred to scammers (43 MILLION CALLS…, 2023). Cybercrime represents a significant threat to Kazakhstan, necessitating the continuous enhancement of cybersecurity measures. Through coordinated efforts by the state, the private sector, and the general public, it is possible to effectively counteract cybercrime and ensure the country's stable development in the digital age.

Enhancing information security: Education, workforce training, and digital literacy

Amid rapid digital advancement and growing cyber threats, Kazakhstan, like most countries worldwide, faces the need to anticipate future challenges in information security. One effective method of strategic planning under such conditions is scenario analysis – an approach enabling the modelling of multiple potential event trajectories, accounting for both internal and external influencing factors. Within this study, three scenarios were developed, conventionally categorised as optimistic, pessimistic, and inertial (Table 4). These reflect different trajectories of digital security development, depending on policy effectiveness, international cooperation levels, civil society engagement, and readiness for innovation.

Scenario	Key Characteristics	Potential Consequences
Optimistic	Adoption of modern legislation addressing global challenges; establishment of a national cyber resilience framework; investment in education and digital literacy; engagement in international assistance and partnerships	Enhanced cybersecurity at all levels; increased trust in digital services; improved international reputation of the country
Pessimistic	Uncontrolled spread of disinformation; frequent cyberattacks targeting critical infrastructure (energy	Political destabilisation; economic losses due to disruptions in digital infrastructure; leakage of

	systems, transport, finance); foreign interference in domestic politics via digital platforms; erosion of trust in public institutions	personal and governmental data
Inertial	Maintenance of the existing model with minimal adjustments; lack of systematic modernisation in information security; limited funding for digital transformation; insufficient human resource development	Vulnerability to emerging threats; delayed response to cyberattacks; stagnation of digital policy and technological lagging

Table 4 – Scenarios for information security development in Kazakhstan

The optimistic scenario envisages proactive government engagement in cybersecurity reforms: enhancing the regulatory framework, implementing national information security standards, and fostering partnerships with international organisations, including the International Telecommunication Union (ITU), United Nations Development Programme (UNDP), and the World Bank. A critical focus area is digital education – integrating cyber hygiene courses into school and university curricula and raising public awareness through information campaigns. The pessimistic scenario is predicated on the risks of weakened state oversight of the digital environment. Amid escalating geopolitical tensions, attacks on Kazakhstan's critical infrastructure are plausible, as witnessed, for instance, in 2022 during mass protests, when hacking interventions targeting government portals were recorded. Another significant threat is the proliferation of politically motivated disinformation through social media platforms. The inertial scenario is the most probable if the status quo persists. This implies that isolated initiatives in the field of information security (IS) may exist but will lack systemic coherence. The failure to modernise technical infrastructure and the low skill levels of personnel will render systems vulnerable to emerging threats, such as AI-driven attacks, phishing, deepfakes, and similar exploits.

Applying scenario analysis to forecast the development of information security in Kazakhstan not only facilitates risk assessment but also enables the formulation of a strategic vision for the future. The nation's resilience to global digital threats hinges on the chosen trajectory – optimistic, pessimistic, or inertial (DAMYANOV et al., 2021). The most effective approach entails institutional modernisation, interstate coordination, and the cultivation of citizens' digital literacy. Conversely, delays or passivity in this domain may result in the loss of

control over the information space, heightened influence of external actors, and destabilisation of the socio-political landscape. Thus, information security must be treated not merely as a technical but as a strategic priority of state policy.

In the context of rapid digital technology advancement and escalating cyber threats, Kazakhstan, like most nations worldwide, faces the imperative of refining its information security policies. Drawing on the findings of scenario analysis, it is prudent to outline a set of strategic and tactical recommendations to strengthen the state's informational sovereignty, enhance institutional cyber resilience, and safeguard citizens' digital security. First and foremost, attention should be directed towards revising and updating existing cybersecurity legislation to address emerging challenges in the digital landscape. This involves aligning legal norms with international standards, particularly those of the EU and the US. Clear regulations must be established for personal data processing, critical infrastructure protection, cyber incident response, and accountability for cybercrimes. Additionally, the creation of a unified coordination body responsible for managing all aspects of information security – including monitoring, analytics, threat response, and strategic planning – should be prioritised. The development of artificial intelligence technologies for cyber threat analysis, fake campaign detection, and botnet identification should be incentivised. AI-driven solutions can automate cyberattack identification processes, thereby improving response times (SMAILOV et al., 2025a; SMAILOV et al., 2025b).

Special attention must be paid to citizens' digital literacy. Mandatory cyber hygiene education should be introduced in school curricula, higher education institutions, and public service training. Open-access online learning platforms and large-scale awareness campaigns to combat fraud, phishing, and disinformation are essential (HARI et al., 2024; KAUSHIK, 2024). Equally important is elevating the digital competency of entrepreneurs and small businesses, which are particularly vulnerable to attacks due to limited cybersecurity resources. State-supported cybersecurity programmes for businesses – including subsidies for protective software, access to 2FA tools, VPNs, and backup solutions – are recommended. A key priority is establishing a system of continuous professional development for IT and information security specialists. State-certified training programmes in partnership with leading technology firms (e.g., Cisco, IBM, Microsoft) should be initiated. The creation of a national cybersecurity school encompassing educational programmes, upskilling courses, and research centres would address the acute shortage of qualified professionals in this field.

The cybersecurity professional shortage in Kazakhstan stems from a combination of limited educational resources and investment in advanced training and research, alongside emigration and global talent competition. The

government's efforts to attract foreign specialists through new visa programs show promise but have yet to fully offset the domestic shortfall. Kazakhstan's educational system, while improving, still demonstrates relatively low expenditure per student, which may impact the quality and breadth of IT and cybersecurity education. This limits the pipeline of locally trained cybersecurity specialists. Additionally, the country faces budgetary constraints that affect investments in cutting-edge research and specialized infrastructure for cybersecurity skill development, hindering the growth of a domestic talent pool prepared to meet modern challenges. There is a documented trend of IT professionals – including cybersecurity specialists – seeking better opportunities abroad or in countries with more mature digital economies. Kazakhstan is actively trying to counter this by introducing programs like the Digital Nomad Residency Visa to attract global IT talent, including cybersecurity experts, yet local talent sometimes also moves out for higher-paying or more advanced roles elsewhere. Kazakhstan has a Digital Nomad Residency Visa specifically for highly skilled IT professionals in fields like AI, big data, and cybersecurity, offering a simplified path to permanent residency (PR). This differs from the Neo Nomad Visa, which is for remote workers and freelancers without a PR pathway.

3Given the transnational nature of information threats, Kazakhstan must actively participate in regional and global cybersecurity initiatives. This includes collaboration with the United Nations (UN), Organisation for Economic Co-operation and Development (OECD), Organization for Security and Co-operation in Europe (OSCE), Europol, INTERPOL, and Central Asian states within the frameworks of the Shanghai Cooperation Organisation (SCO) and Collective Security Treaty Organization (CSTO). Participation in developing unified cyber incident response standards and real-time threat intelligence-sharing mechanisms is vital.

Kazakhstan has recently taken a significant step in its active participation in regional and global cybersecurity initiatives by signing the United Nations Convention against Cybercrime (2024). This convention, adopted by the UN General Assembly in December 2024 and opened for signature starting October 25, 2025, in Hanoi, Vietnam, is the first comprehensive international treaty addressing crimes committed through digital technologies. By joining this Convention, Kazakhstan commits to strengthening international cooperation in combating cybercrime, including offenses like hacking, online fraud, terrorism financing, and human trafficking facilitated by ICT systems. The Convention expands jurisdictional powers, allowing Kazakhstan not only to prosecute crimes within its territory but also those affecting its citizens or entities abroad. It also introduces expedited procedures for preserving and exchanging electronic evidence among law enforcement agencies across borders. Additionally,

Kazakhstan has hosted international conferences on countering cybercrime, partnering with organizations such as the UNODC, UNICEF, the OSCE, Interpol, and leading IT companies to share expertise and strengthen collective cybersecurity resilience.

It is imperative to actively develop the national information space by creating media platforms aligned with the country's cultural values. The state must support the production of national content, stimulate the development of local social networks, video hosting platforms, and news services. Standards for content transparency, countering fake news, and disinformation should be implemented. Furthermore, mechanisms for the legislative regulation of social media platforms should be revised, including provisions for holding entities accountable for inciting hatred, promoting violence, or disseminating false information that threatens national security. Mandatory information security audits for both public and private organisations should be introduced. This will enable timely identification of vulnerabilities and the implementation of effective protective mechanisms. It is advisable to cultivate a culture of penetration testing – simulating real cyberattacks with the involvement of ethical hackers. A unified national cyber incident response protocol should be established, with clearly defined responsibilities, action guidelines in the event of attacks, and algorithms for interagency information exchange. In cases of critical threats, provisions must be made for rapid mobilisation of security forces, isolation of vulnerable systems, and activation of backup channels. The implementation of these recommendations will significantly enhance Kazakhstan's information security in both the short and long term. The synergy between technical solutions, institutional modernisation, educational initiatives, and international cooperation will form the foundation of an effective strategy to counter contemporary information threats. In the digital age, national security begins with the security of its information space – and Kazakhstan possesses all the necessary resources to ensure its robust protection.

DISCUSSION

In the context of a globalised society, information security has acquired a new dimension, defined not only by technical threats but also by political, social, and legal aspects. Data analysis has led to the conclusion that information security is a multidimensional phenomenon, directly linked to widespread digitalisation, the transformation of cyberspace, and the intensification of malicious activities at various levels – from local to international. The findings confirm that the most significant threats to information security today include attacks on critical information infrastructure, manipulation of personal data, and breaches of data confidentiality, integrity, and availability. These conclusions align with the arguments presented in the work of Al Hayajneh et al. (2023), which emphasised

that the evolution of information security strategies is a response to escalating risks in the global information era. The authors demonstrated that traditional security approaches no longer provide adequate protection and require the integration of risk-oriented strategies. The study also revealed that digital transformations, particularly the proliferation of the Internet of Things (IoT), serve not only as a catalyst for economic development but also as a factor amplifying vulnerabilities. This observation was corroborated by the findings of Ande et al. (2020), who noted that the increasing number of network-connected devices expands the potential attack surface. Our results indicate that poorly secured IoT devices often act as entry points for intrusions, which is consistent with the position of Djenna et al. (2021), who characterised IoT as an element of the "Internet of Threats". Special attention was given to analysing the regulatory framework governing information security. It was established that many countries still lack sufficiently developed legal mechanisms for personal data protection. These findings resonate with the research of Calzada (2022), which examined legislative developments in China, particularly the Personal Information Protection Law (PIPL). The author highlighted that even in highly digitalised states, privacy remains a politically and socially sensitive issue. The analysis identified an uneven distribution of information security levels between highly digitalised and developing nations. In the latter, insufficient funding, low cyber literacy, and inadequate institutional safeguards create a conducive environment for cyberattacks. This conclusion aligns with the observations of Chang and Coppel (2020), who demonstrated that fostering public cyber awareness requires long-term efforts, systemic reforms, and international support.

The study also revealed that global information security cannot be isolated from political processes. The results confirmed that issues of information sovereignty, data control, and cyber diplomacy are increasingly leveraged in interstate relations. This fully corresponds with the conclusions of Cavelty and Wenger (2020), who examined cybersecurity through the lens of complex political interactions, where technology, science, and policy are interdependent. Furthermore, the research identified limitations in existing risk assessment methodologies for information security. This aspect echoes the work of Bhutta et al. (2021), which explored blockchain technology as an innovative tool for ensuring data integrity and enhancing trust in digital transactions. However, the authors stressed that even such promising technologies are not without vulnerabilities, and their widespread adoption requires extensive research and regulatory support.

In the work of Getman et al. (2020), it was emphasised that information security extends beyond technical data protection and encompasses sociocultural mechanisms of fostering information resilience. This aligned with the findings of

a study that also identified media literacy and critical thinking as key factors in enhancing the security of the information space. Particularly relevant was the issue of trust in information sources, which forms the foundation of resilience to disinformation in the context of hybrid threats. Similarly, González-Granadillo et al. (2021) focused on the role of Security Information and Event Management (SIEM) systems in safeguarding critical infrastructure. The authors concluded that flexible and adaptive systems are required for real-time incident monitoring. In the context of this study, a similar position was corroborated by findings on the necessity of continuously updating protective measures in response to emerging challenges. However, it was noted that implementing such solutions in less developed countries faces financial, personnel, and infrastructural constraints – an aspect that was somewhat underestimated in the aforementioned work.

The publication by Hren et al. (2023) highlighted the multidimensional nature of information security, which includes legal, organisational, technical, and social aspects. This fully aligned with the approaches applied in the study, particularly regarding the interplay between institutional policies, legal regulations, and users' information behaviour culture. The research also revealed that the development of national information security strategies should be based on context-sensitive principles, consistent with the theses presented by Hren et al. In their work, Judijanto et al. (2023) examined the role of corporate architecture in mitigating cyber threats. The authors emphasised the need for integrated risk management systems at all levels of enterprise operations. The study confirmed this thesis, demonstrating that the effectiveness of protection significantly increases when information security is treated as a component of overall management strategy. However, it was found that in many organisations, strategic security planning remains fragmented, leading to vulnerabilities even when technical safeguards are in place. Li and Liu (2021), in their review of cyberattacks and cybersecurity trends, outlined the contemporary threat landscape, highlighting the rise of ransomware, phishing, and attacks on cloud services. The trends identified in this study fully corresponded with these observations. Particular attention was paid to the growing importance of data security in cloud environments, which are utilised by both public and private entities. However, the study also revealed that users often lack sufficient awareness of protective mechanisms in such environments, necessitating awareness-raising campaigns.

Analysing the development of the UN Guiding Principles on Business and Human Rights, Ruggie (2020) underscored the importance of responsible corporate governance in upholding digital rights. This perspective allowed information security to be viewed not merely as a technical or administrative issue but as a matter of ethics and corporate accountability. The study found that

information security breaches often have direct consequences for human rights – ranging from privacy violations to threats to reputation, health, or even life. Information security must become an integral part of the discourse on digital human rights. The study by Rantanen et al. (2020) examined workplace safety in the context of globalisation, particularly in hybrid work environments. The authors highlighted new risks faced by employees due to remote access to corporate resources. These conclusions were reflected in the analysis of workplace security, which was also part of the study's scope. It was found that most organisations lack clear protocols for ensuring information security in remote work settings, posing risks to management quality, confidentiality, and business process stability.

Safitra et al. (2023) proposed a conceptual model for future security, stressing the need for proactive responses to evolving threats. The results indicated that the rapid pace of digital transformation has not been matched by a corresponding level of information security. This imbalance was particularly evident in the public and education sectors. Similar findings were reported in the study by Sarbu et al. (2021), which demonstrated that during the COVID-19 pandemic and the abrupt shift to remote work and learning, information security was deprioritised by many governments. This situation introduced additional infrastructural vulnerabilities, as also confirmed by the study's results. Crucially, it was found that most organisations still rely on reactive rather than proactive cybersecurity models. Sarker et al. (2021) noted that the implementation of artificial intelligence could significantly enhance anomaly detection and attack prediction, though such solutions require substantial investment and expertise. The current study also found that only a limited number of institutions had integrated machine learning systems into data protection processes. The research supported the hypothesis that an integrated information security ecosystem – combining technology, regulatory frameworks, and human factors – is essential. Similar propositions were reflected in the work of Sobb et al. (2020), who analysed security challenges in supply chain logistics and advocated for a systemic approach to security. The study further confirmed that the most secure entities were those implementing comprehensive information security policies encompassing not only IT solutions but also staff training, audits, and crisis planning. A divergence in findings was observed when comparing results with the work of Taherdoost et al. (2022), where the authors emphasised the universality of international information security standards. The analysis revealed that adopting such standards does not always guarantee a high level of security. The primary issue remained the formalistic implementation of standards without proper monitoring and oversight. This suggested that the efficacy of security standards depends less on their existence and more on the depth of

implementation and the organisation's cybersecurity culture. Simultaneously, the data aligned with the findings of Wenhua et al. (2023), who highlighted the growing role of blockchain technologies in ensuring data transparency and integrity, particularly in healthcare. This study also found blockchain to be highly effective in safeguarding critical public sector data, though its integration remains limited due to technical complexity and high implementation costs.

CONCLUSIONS

As a result of the conducted research, several key aspects concerning information security in the Republic of Kazakhstan have been identified. The primary objective was to examine the current state of information security, analyse national and international approaches to its provision, and explore the challenges Kazakhstan faces in this domain. The study yielded a number of significant findings that confirmed the relevance of the topic and outlined specific directions for further action. One of the key findings of the research is that Kazakhstan has a clearly defined information security strategy enshrined in regulatory and legal frameworks, particularly in the Digital Transformation Concept for 2023-2029. This enables the country to focus efforts on developing IT infrastructure, enhancing cybersecurity, and improving the digital literacy of its citizens. According to survey data, approximately 74% of respondents believe that national cybersecurity development programmes are effective, though 56% of them highlight the need for more intensive work in personnel training. The study also identified significant challenges in cybersecurity education, particularly a shortage of qualified professionals. The lack of sufficient specialists, especially in critical infrastructure, poses one of the greatest threats to national security. Only 45% of respondents indicated having access to high-quality cybersecurity training programmes. This supports the conclusion that new educational initiatives aimed at upskilling professionals in this field are necessary.

Regarding the current level of cybersecurity awareness among Kazakhstani citizens, survey results revealed that the majority of respondents (80%) possess basic knowledge of cybercrime and information security threats. However, only 43% reported regularly using protective measures such as antivirus software or VPNs, indicating the need for broader adoption of cyber hygiene practices among the population. Another key finding is the analysis of external and internal threats facing the country. Respondents highlighted serious risks from cyberattacks, social media manipulation, and information misuse. Among external threats, information expansion and the use of digital technologies for political pressure deserve particular attention, demonstrating the relevance of these issues in the national cybersecurity strategy. Additionally, external threats, including cyberattacks by foreign states and attacks on critical infrastructure, have

a substantial impact on the country's economy and stability. In recent years, Kazakhstan has experienced several large-scale cyber incidents, such as attacks on banks and energy systems, which had significant economic consequences. These incidents underscore the importance of investments in cyber defence and critical infrastructure protection. In the context of international cooperation, Kazakhstan actively collaborates with international organisations and other countries in cybersecurity. However, survey data indicates that only 60% of respondents consider such cooperation sufficiently effective, suggesting room for improvement in these relations and the expansion of partnerships in combating cybercrime.

Among the recommendations, the need to enhance the legal framework for cybersecurity, strengthen IT security personnel training, and implement more effective digital literacy programmes for the population should be emphasised. Additionally, a crucial step would be the establishment of a national cyber threat early warning system to minimise risks from cyberattacks and enable rapid response to potential threats.

Further research in this field should focus on a deeper examination of international cooperation practices and information exchange with other states. Given that cybercrime is borderless, international collaboration is a critical factor in effectively countering cyber threats. Equally important is the development of methods and technologies for monitoring and predicting cyber threats at the national level.

Certain limitations of the study relate to restricted access to some confidential information, as well as the difficulty of assessing the effectiveness of specific policies due to a lack of long-term data. Furthermore, the research does not cover all aspects of cybersecurity related to specific technologies or enterprises, which also represents an important direction for future studies. In general, the study demonstrates that Kazakhstan has taken certain steps towards ensuring cybersecurity. However, to achieve greater effectiveness, both institutional and practical measures in this field must be strengthened, particularly through improved educational initiatives and human resource development.

Funding

The article was prepared based on research funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (grant No. BR24993082 "Comprehensive Study of the Humanitarian Aspects of Kazakhstan's Information Security and Components of 'Soft Power' in Ensuring Sustainable Development and the Consolidation of Kazakhstani Society").

REFERENCES

43 million calls blocked: Kazakhstanis gave billions to scammers. (2023). https://tengrinews.kz/crime/zablokirovano-43-milliona-zvonkov-kazahstantsyi-otdali-521683/

Al Hayajneh, A., Thakur, H. N., & Thakur, K. (2023). The evolution of information security strategies: A comprehensive investigation of INFOSEC risk assessment in the contemporary information era. *Computer and Information Science*, *16*(4), 1. https://doi.org/10.5539/cis.v16n4p1

Allahverdiyev, E. N. (2023). The selection of transmitters using fuzzy logic method. *Technologies and Engineering, 24*(2), 9-14. https://doi.org/10.30857/2786-5371.2023.2.1

Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2019). Internet of Things: Evolution and technologies from a security perspective. *Sustainable Cities and Society*, *54*, 101728. https://doi.org/10.1016/j.scs.2019.101728

Apakhayev, N., Omarova, A. B., Kussainov, S., Nurahmetova, G. G., Buribayev, Y. A., Khamzina, Z. A., Kuandykov, B., Tlepina, S. V., & Kala, N. S. (2018). Review on the outer space legislation: Problems and prospects. *Statute Law Review, 39*(3), 258-265. https://doi.org/10.1093/slr/hmx010

Azanbay, K. (2024). Innovative technologies as a factor of information security of the Republic of Kazakhstan. *Information Systems Engineering*, *29*(2), 523–532. https://doi.org/10.18280/isi.290213

Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., Song, H., Alshamari, M., & Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security. *IEEE Access*, *9*, 61048–61073. https://doi.org/10.1109/access.2021.3072849

Calzada, I. (2022). Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). *Smart Cities*, *5*(3), 1129–1150. https://doi.org/10.3390/smartcities5030057

Cavelty, M. D., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Chang, L. Y., & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers & Security*, *97*, 101959. https://doi.org/10.1016/j.cose.2020.101959

Committee of Information Security of the Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan. (2024). Cybersecurity issues. Recommendations.

https://www.gov.kz/memleket/entities/infsecurity/press/article/details/147792?lang=en

Damyanov, D., Kavaldjieva, K., Vlahova, B., & Lazarov, V. (2021). Innovation Process and Degree of Innovation and Innovation Activity. In *International Conference on High Technology for Sustainable Development, HiTech 2021 - Proceedings.* Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/HiTech53072.2021.9614233

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things meet Internet of Threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), 4580. https://doi.org/10.3390/app11104580

Duisenbekuly, A., Kulbay, B., Bigeldiyeva, Z., Zhakipbekova, D., & Daurbayeva, M. (2024). Food security in Kazakhstan and Azerbaijan: Challenges and strategies for economic and sustainable development. *International Journal on Food System Dynamics*, *15*(3), 267–277. https://doi.org/10.18461/ijfsd.v15i3.k5

European Commission. (2025). The cybersecurity strategy. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

Getman, A. P., Danilyan, O. G., Dzeban, A. P., Kalinovsky, Y. Y., & Hetman, Y. A. (2020). Information security in modern society: Sociocultural aspects. *Amazonia Investiga*, *9*(25), 6–14.

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), 4759. https://doi.org/10.3390/s21144759

Hari, S. S., Porkodi, S., Saranya, R., & Vijayakumar, N. (2024). Intelligent model to improve the efficacy of healthcare content marketing by auto-tagging and exploring the veracity of content using opinion mining. *International Journal of Electronic Marketing and Retailing, 15*(2), 240-260. https://doi.org/10.1504/IJEMR.2024.136978

Hren, L., Karpeko, N., Kopanchuk, O., Strelbitsky, M., & Tohobytska, V. (2023). Substantive essence and components of the societal phenomenon "Information Security" in the age of information society. In O. Radchenko, V. Kovach, I. Semenets-Orlova, & A. Zaporozhets (Eds.), *National Security Drivers of Ukraine: Information Technology, Strategic Communication, and Legitimacy* (pp. 75–91). Springer. https://doi.org/10.1007/978-3-031-33724-6_5

Iasechko, S., Haliantych, M. K., Skomorovskyi, V. B., Zadorozhnyi, V., Obryvkina, O., & Pohrebniak, O. (2020). Contractual relations in the information sphere. *Systematic Reviews in Pharmacy, 11*(8), 301–303. https://doi.org/10.31838/srp.2020.8.46

Judijanto, L., Hindarto, D., Wahjono, S. I., & Djunarto, N. (2023). Edge of enterprise architecture in addressing cyber security threats and business risks. *International Journal Software Engineering and Computer Science (IJSECS)*, *3*(3), 386–396. https://doi.org/10.35870/ijsecs.v3i3.1816

Kaushik, D. (2024). Policy Responses To Fake News On Social Media Platforms: A Law And Economics Analysis. *Statute Law Review, 45*(1), hmae013. https://doi.org/10.1093/slr/hmae013

Kozhan, A. A., Yilmaz, S., Osserbayev, Y. N., Shadinova, G. A., & Dosaliyev, T. K. (2025). The digitalization era: Philosophical aspects of technological civilization in modern Kazakhstan. *Bulletin of the Karaganda University History. Philosophy Series*, *11730*(1), 286–299.

KZ-CERT. (2024). National computer emergency response team of Kazakhstan. https://www.cybersecurityintelligence.com/kz-cert-2759.html

Li, X., Anukul, T., & Ying, F. (2024). Cross-platform adaptation of algorithmic editing techniques. *Bulletin of Cherkasy State Technological University, 29*(2), 45-56. https://doi.org/10.62660/bcstu/2.2024.4510.62660/2.2024.45

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Mehla, A., & Mehla, L. (2024). The Telecommunications Act, 2023: Solidarity Between Democracy and Totalitarianism. *Statute Law Review, 45*(2), hmae032. https://doi.org/10.1093/slr/hmae032

Myrzakhmetov, A. Zh., Khlebnikov, I. D., Rezvushkina, T. A., & Karaseva, N. V. (2020). Regulatory framework for the formation of information culture of modern Kazakhstan youth. *Bulletin of Karaganda University. Series History. Philosophy*, *99*(3), 114–127.

National Cybersecurity Strategy. (2023). https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Nauryzbaeva, A., Nepshina, V., & Muratova, D. (2024). Development of the innovation ecosystem in the Republic of Kazakhstan. *Economic Series of the Bulletin of the L.N. Gumilyov ENU*, *3*, 193–208. https://doi.org/10.32523/2789-4320-2024-3-193-208

Nussipova, A., Aliyarov, E., Kabilova, R., Karymsakova, K., & Nuralina, B. (2023). Pandemic, hoaxes and information security of Kazakhstan. *Journal of Information Policy*, *13*, 140–158. https://doi.org/10.5325/jinfopoli.13.2023.0011

Omirgazy, D. (2024, January). Kazakhstan registers significant attempts of cyber-attacks in 2023. *The Astana Times*.

https://astanatimes.com/2024/01/kazakhstan-registers-significant-attempts-of-cyber-attacks-in-2023/

Oralova, S. S. (2022). The main trends in the formation of the internet space and information society in Kazakhstan. *Economy Strategy and Practice*, *17*(1), 50–61. https://doi.org/10.51176/1997-9967-2022-1-50-61

Order of the President of the People's Republic of China No. 84 "Data Security Law of the People's Republic of China". (2021). http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html

Rantanen, J., Muchiri, F., & Lehtinen, S. (2020). Decent work, ILO's response to the globalization of working life: Basic concepts and global implementation with special reference to occupational health. *International Journal of Environmental Research and Public Health*, *17*(10), 3351. https://doi.org/10.3390/ijerph17103351

Resolution of the Government of the Republic of Kazakhstan No. 269 "On Approval of the Concept of Digital Transformation, Development of the Information and Communication Technology Industry and Cybersecurity for 2023-2029". (2023). https://adilet.zan.kz/rus/docs/P2300000269

Ruggie, J. G. (2020). The social construction of the UN Guiding Principles on Business and Human Rights. In S. Deva & D. Birchall (Eds.), *Research Handbook on Human Rights and Business* (pp. 63–86). Edward Elgar Publishing. https://doi.org/10.4337/9781786436405.00009

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369. https://doi.org/10.3390/su151813369

Sarbu, R., Alpopi, C., Burlacu, S., & Diaconu, S. (2021). Sustainable urban development in the context of globalization and the health crisis caused by the COVID-19 pandemic. *SHS Web of Conferences*, *92*, 01043. https://doi.org/10.1051/shsconf/20219201043

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science*, *2*, 173. https://doi.org/10.1007/s42979-021-00557-0

Seidakhmetova, F., Pasekova, M., Sarygulova, R., & Sholpanbayeva, K. Zh. (2023). Training of specialists in the field of information security. *Statistics, Accounting and Auditing*, *89*(2), 40–46.

Smailov, N., Akmardin, S., Ayapbergenova, A., Ayapbergenova, G., Kadyrova, R., & Sabibolda, A. (2025a). Analysis of VLC efficiency in optical wireless communication systems for indoor applications. *Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 15*(2), 135–138. https://doi.org/10.35784/iapgos.6971

Smailov, N., Kadyrova, R., Abdulina, K., Uralova, F., Kubanova, N., & Sabibolda, A. (2025b). Application of facial recognition technologies for enhancing control in information security systems. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska, 15*(3), 55–58. https://doi.org/10.35784/iapgos.7073

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply Chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics*, *9*(11), 1864. https://doi.org/10.3390/electronics9111864

State Technical Service. (2025). National Coordination Center for Information Security (NCCIS). https://sts.kz/en/nkcib

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards – A review and comprehensive overview. *Electronics*, *11*(14), 2181. https://doi.org/10.3390/electronics11142181

United Nations Convention against Cybercrime. (2024). https://www.unodc.org/unodc/cybercrime/convention/home.html

Urumkulova, N. (2022). Spiritual and moral formation of young people in modern scientific and technical development of society. *Bulletin of the Jusup Balasagyn Kyrgyz National University, 14*(3), 226-232.

Wenhua, Z., Qamar, F., Abdali, T. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: Security issues, healthcare applications, challenges and future trends. *Electronics*, *12*(3), 546. https://doi.org/10.3390/electronics12030546

Zabikh, S. (2020). International experience of legal support of information security and the possibilities for its application in the Republic of Kazakhstan. *Political Science Review*, *3*, 71–85. https://doi.org/10.14746/pp.2020.25.3.6

Zhanzhumenov, R., Sargazin, Zh., & Esdauletov, N. (2022). Information policy in mass media space: case study of central Asia. *Bulletin of the Jusup Balasagyn Kyrgyz National University, 14*(3), 36-43.

Zhaparalina, B., Sheryazdanova, K., Kakenova, G., & Aliyeva, S. (2024). The influence of information cooperation in Central Asia on the interests and foreign policy of the Republic of Kazakhstan. *Journal of Information Policy*, *14*, 132–160. https://doi.org/10.5325/jinfopoli.14.2024.0004

Zhetpisbayev, B. A., Baisalova, G. T., Shadiyev, K. K., Khamzin, A. S., Buribayev, Y. A., & Khamzina, Z. A. (2017). Legal support of the process of Kazakhstan accession to the OECD: Potential for improving quality of individual's labour rights regulation. *Journal of Advanced Research in Law and Economics, 8*(7), 2302-2307. https://doi.org/10.14505//jarle.v8.7(29).31

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET