IRSTI 06.77.75 https://doi.org/10.26577/JGEM20257949

Zh. Aliyeva[1], Zh. Baden[1], I. Akbar[1]*, Z. Myrzaliyeva[2], M. Udahogora[3]

[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[2]South Kazakhstan Pedagogical University named after Uzbekali Zhanibekov, Shymkent, Kazakhstan
[3]Rwanda Rural Rehabilitation Initiative NGO, Kigali, Rwanda
*e-mail: akbar.imanaly@gmail.com

CYBERSECURITY IN KAZAKHSTAN'S TOURISM SECTOR: CHALLENGES AND SOLUTIONS IN THE PROTECTION OF PERSONAL DATA

The digital transformation of the tourism industry has significantly improved service efficiency, booking convenience, and customer experience. However, the widespread use of online platforms, electronic payments, and mobile applications has also introduced substantial cybersecurity risks, particularly concerning the protection of travelers' personal and financial data. This paper explores the key cybersecurity threats facing the global tourism industry, with a specific focus on Kazakhstan's emerging digital travel infrastructure. The study employs a multi-method approach, including analysis of cyber threats, a comparative review of international data protection regulations, evaluation of technical and organizational security practices, and an empirical survey involving tourism and aviation sector professionals in Kazakhstan. The findings indicate that phishing attacks, payment data breaches, and malware are among the most common threats affecting tourism businesses. These vulnerabilities are often exacerbated by outdated security systems, insufficient staff training, and limited awareness of best practices in data protection. Through a comparative analysis of cybersecurity legislation in Kazakhstan, the European Union (GDPR), the United States (CCPA), and Singapore (PDPA), the study highlights significant regulatory gaps and enforcement limitations within Kazakhstan's legal framework. Survey results further reveal a lack of preparedness in small and medium-sized tourism enterprises, where modern security technologies and training programs are not widely adopted. Based on these insights, the paper recommends implementing multi-factor authentication, encryption protocols, regular cybersecurity audits, and employee awareness initiatives. The use of advanced technologies such as artificial intelligence and blockchain is also encouraged to enhance threat detection and data integrity. This research underscores the urgent need for a robust cybersecurity strategy in the tourism industry. By strengthening data protection measures and aligning with global standards, tourism companies can safeguard consumer trust, reduce financial risks, and support the secure digital growth of the travel sector.

Keywords: cybersecurity, tourism industry, personal data protection, multi-factor authentication, SWOT analysis, artificial intelligence, Kazakhstan.

Ж.Н. Алиева[1], Ж.С. Баден[1], И. Акбар[1]*,
З.Қ. Мырзалиева[2], М. Удахогора[3]

[1]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
[2]Өзбекәлі Жәнібеков атындағы Оңтүстік Қазақстан педагогикалық университеті, Шымкент, Қазақстан
[3]Руанда ауылдық жерлерін қалпына келтіру бастамасы үкіметтік емес ұйымы, Кигали, Руанда
*e-mail: akbar.imanaly@gmail.com

Қазақстан туризміндегі киберқауіпсіздік: жеке деректерді қорғау мәселелері мен шешімдер

Туризм индустриясының цифрлық трансформациясы қызмет көрсету тиімділігін, брондау ыңғайлылығын және тұтынушы тәжірибесін айтарлықтай жақсартты. Алайда онлайн платформалар, электронды төлемдер және мобильді қосымшалардың кең таралуы киберқауіпсіздікке қатысты елеулі қатерлерді, әсіресе саяхатшылардың жеке және қаржылық деректерін қорғау мәселесін алға тартты. Бұл мақалада жаһандық туризм индустриясына төнетін негізгі киберқауіптер қарастырылып, Қазақстандағы цифрлық туристік инфрақұрылымның қалыптасуына ерекше назар аударылады. Зерттеу көп әдісті тәсілге негізделген: киберқауіптерді талдау, халықаралық деректерді қорғау ережелеріне шолу, техникалық және ұйымдастырушылық қауіпсіздік тәжірибелерін бағалау, сондай-ақ Қазақстандағы туризм және авиация салаларының мамандары арасында жүргізілген эмпирикалық сауалнама нәтижелері қамтылған. Зерттеу нәтижелері фишинг шабуылдары, төлем деректерінің бұзылуы және зиянды бағдарламалардың туризм кәсіпорындарына ең жиі әсер ететін қауіптердің қатарына жататынын көрсетеді. Бұл осалдықтар көбінесе ескірген қауіпсіздік жүйелерімен, персоналдың жеткіліксіз дайындық деңгейімен және деректерді қорғаудағы озық тәжірибелер туралы білімнің аздығымен байланысты. Қазақстан, Еуропалық Одақ (GDPR), АҚШ (CCPA) және Сингапур (PDPA) арасындағы киберқауіпсіздік заңнамаларының салыстырмалы талдауы Қазақстанның құқықтық жүйесінде елеулі реттеушілік олқылықтар мен бақылау тетіктерінің әлсіздігін айқындайды. Сауалнама нәтижелері шағын және орта туристік кәсіпорындарда заманауи қауіпсіздік технологиялары мен оқыту бағдарламаларының кеңінен енгізілмегендігін көрсетеді. Осыған байланысты мақалада көп факторлы аутентификация, шифрлау хаттамалары, тұрақты киберқауіпсіздік аудиттері және қызметкерлер арасында ақпараттандыру бастамаларын енгізу ұсынылады. Сонымен қатар, жасанды интеллект пен блокчейн сынды заманауи технологияларды қолдану қауіп-қатерді анықтау мен деректердің тұтастығын қамтамасыз етуге жәрдемдеседі. Бұл зерттеу туризм индустриясында пәрменді киберқауіпсіздік стратегиясын әзірлеудің өзектілігін атап көрсетеді. Деректерді қорғау шараларын күшейту және жаһандық стандарттармен үйлестіру арқылы туристік компаниялар тұтынушылар сенімін сақтап, қаржылық тәуекелдерді азайтып, саланың қауіпсіз цифрлық дамуына жол аша алады.

Түйін сөздер: киберқауіпсіздік, туризм индустриясы, жеке деректерді қорғау, көп факторлы аутентификация, SWOT-талдау, жасанды интеллект, Қазақстан.

Ж.Н. Алиева[1], Ж.С. Бәден[1], И. Акбар[1*],
З.К. Мырзалиева[2], М. Удахогора[3]

[1]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
[2]Южно-Казахстанский педагогический университет им. Өзбекәлі Жәнібеков, Шымкент, Казахстан
[3]НПО «Инициатива по восстановлению сельских районов Руанды», Кигали, Руанда
*e-mail: akbar.imanaly@gmail.com

Кибербезопасность в туризме Казахстана: проблемы и решения в области защиты персональных данных

Цифровая трансформация туристической индустрии значительно повысила эффективность обслуживания, удобство бронирования и качество клиентского опыта. Однако широкое распространение онлайн-платформ, электронных платежей и мобильных приложений привело к существенным киберрискам, особенно в вопросах защиты персональных и финансовых данных путешественников. В данной статье рассматриваются основные угрозы кибербезопасности, с которыми сталкивается мировая туристическая отрасль, с особым акцентом на развивающуюся цифровую инфраструктуру туризма в Казахстане. В исследовании используется многоуровневый методологический подход, включающий анализ киберугроз, сравнительный обзор международных нормативных актов по защите данных, оценку технических и организационных мер безопасности, а также эмпирическое анкетирование специалистов туристической и авиационной сфер Казахстана. Результаты исследования показывают, что фишинг-атаки, утечки данных платежных систем и вредоносное программное обеспечение являются одними из наиболее распространённых угроз для туристических компаний. Уязвимости усугубляются использованием устаревших систем безопасности, недостаточной подготовкой персонала и низким уровнем осведомлённости о лучших практиках в сфере защиты данных. Сравнительный анализ законодательства в области кибербезопасности Казахстана, Европейского союза (GDPR), США (CCPA) и Сингапура (PDPA) выявляет значительные пробелы в регулировании и недостаточную эффективность механизмов правоприменения в казахстанской правовой системе. Результаты опроса также указывают на низкий уровень готовности среди малых и средних туристических предприятий, где современные технологии защиты и программы обучения практически не внедряются. На основании полученных данных в статье предлагается внедрение многофакторной аутентификации, протоколов шифрования, регулярных аудитов кибербезопасности и инициатив по повышению осведомлённости сотрудников. Также рекомендуется использование передовых технологий, таких как искусственный интеллект и блокчейн, для повышения эффективности обнаружения угроз и обеспечения целостности данных. Данное исследование подчёркивает срочную необходимость разработки комплексной стратегии кибербезопасности в туристической отрасли. Усиление мер по защите данных и приведение национальных стандартов в соответствие с международными позволит туристическим компаниям укрепить доверие потребителей, снизить финансовые риски и обеспечить безопасное цифровое развитие сектора.

Ключевые слова: кибербезопасность, туристическая индустрия, защита персональных данных, многофакторная аутентификация, SWOT-анализ, искусственный интеллект, Казахстан.

Introduction

Today, the tourism industry is rapidly developing thanks to digital technology, which also demands cybersecurity and the protection of travelers' data. In Kazakhstan, the number of online payments, online bookings, and digital tourism services is steadily increasing. According to the Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan, nearly 70% of travelers booked hotels and tickets online in 2023. On the other hand, cyberattacks are becoming more frequent. In 2022, the National Security Committee of the Republic of Kazakhstan reported nearly 2,000 cyberattacks targeting both public and private tourism services, including hotel and travel agency databases (del Mar Alonso-Almeida & Giglio, 2024).

Cyber threats in tourism have become a major global issue. According to IBM Security Survey data, the tourism sector ranks among the ten most vulnerable industries to cyberattacks, following the banking and healthcare sectors (Roy et al., 2023). The main threats include phishing attacks, theft of financial data, and unauthorized access to hotel data storage systems. In 2018, Marriott International announced that the personal data of 500 million customers had been compromised, including passport information and credit card numbers (Perlroth et al., 2018). This led to legal proceedings against the hotel chain and significant financial losses.

Overall, cybersecurity in the tourism sector has become the subject of growing research, particularly concerning the protection of personal data, financial information, and the prevention of data breaches – topics that are increasingly discussed at the governmental level. In Kazakhstan, this issue has received special attention under the *Digital Kazakhstan* initiative, which aims to provide secure digital services with *the approval of the State Program Digital Kazakhstan in 2017*. This article examines the key aspects of cybersecurity in the tourism and travel sector both in Kazakhstan and globally. It addresses the most common cyber threats, including phishing schemes, malware attacks, and the exposure of personal data. It also explores how the hospitality and aviation industries manage data security (Thealla et al., 2024).

Literature review

International studies highlight how vulnerable the tourism sector is due to the vast amount of personal data collected online. According to an article by Alexandros Paraskevas, data encryption and multi-factor authentication are crucial for protecting consumers (Paraskevas, 2022). Blockchain technology is also recommended for the secure storage of bookings and transactions.

The tourism sector actively uses information technologies for booking, payments, and processing travelers' personal information in the context of global digitalization. However, due to the growing reliance on digital services, the tourism industry remains vulnerable to cyber threats. This section reviews previous research on cybersecurity in the tourism industry, identifies the main risks, explores current methods for protecting personal information, and analyzes responses to cyberattacks based on both local and international practices (Florido-Benítez, 2025).

Phishing attacks, breaches of booking systems, theft of payment data, and leaks of personal information are among the most common threats in the tourism industry, according to cybersecurity research. IBM Security reports (2023) show that over 60% of cyberattacks in the travel and tourism sector are aimed at stealing consumer data, which is later used in fraudulent schemes. A study by Cornell University and FreedomPay revealed that nearly 31% of hospitality organizations experienced data breaches in 2023, with 89% facing multiple attacks within the same year (Ghaderi, Beal, & Houanti, 2024). These breaches often led to the exposure of personal information, disrupted guest services, and resulted in substantial financial damage.

At the international level, passenger data is protected through multi-factor authentication (MFA), data encryption, suspicious activity monitoring systems, and artificial intelligence tools for threat assessment (Williamson & Curran, 2021). For example, major airlines such as Delta and Lufthansa have adopted blockchain technology to secure bookings and transactions (Thealla et al., 2024).

Kazakhstani companies are also beginning to implement modern data protection methods. For instance, hotel chains such as Rixos and Hilton Kazakhstan have improved customer data protection by using multi-level encryption, while Air Astana has introduced a cyber threat monitoring system (Мосунова, 2024). However, due to a shortage of experts and financial resources, most small and medium-sized travel agencies in Kazakhstan do not use advanced technologies.

The General Data Protection Regulation (GDPR) of the European Union requires travel agencies to ensure a high level of protection for their customers' data and strictly regulates access to it. According to Jaeyoon Baik, a similar regulation in the United States, the California Consumer Privacy Act (CCPA), was introduced to impose strict penalties for data protection violations (Baik, 2020).

In Kazakhstan, the Law on Personal Data and Their Protection governs cybersecurity issues; however, it does not provide specific guidelines for the travel and tourism sector. According to an analysis by N. Satkanov, Kazakhstan needs to develop its security regulations for travel agencies that are comparable to the GDPR (Syzdykova et al., 2024).

Based on a review of scientific literature, cyber threats are becoming increasingly significant in the tourism industry, both in Kazakhstan and worldwide. Global experience demonstrates the effectiveness of systems such as blockchain, multi-factor authentication, and data encryption (Zishan & Russell, 2024). However, Kazakhstan still needs to adopt modern security technologies, enhance staff awareness, and strengthen legal regulation.

Research Methodology

This study employed a rigorous methodological approach that included surveys, comparative analysis of global practices, evaluation of the effectiveness of current personal data protection measures, and analysis of cyber threats. These empirical methods enabled the collection of objective information on the state of cybersecurity in the tourism sector in Kazakhstan and other countries, the identification of key issues, and the development of practical recommendations for addressing them. To identify the main cyber threats facing the tourism sector, the study thoroughly examined reports from global organizations such as IBM Security X-Force, the European Cybersecurity Commission, and the International Air Transport Association (IATA), as well as data from Kazakhstan's National Cybersecurity Center.

This study employed a comprehensive and multi-faceted methodological approach to explore the current state of cybersecurity in the tourism industry and to assess the effectiveness of data protection practices. A combination of qualitative and quantitative methods was used to ensure a thorough understanding of the research problem and to develop practical recommendations.

First, a detailed analysis of cyber threats and vulnerabilities within the tourism sector was conducted. This included reviewing international reports from trusted institutions such as IBM Security X-Force, the European Cybersecurity Commission, and the International Air Transport Association (IATA). In addition, national statistics and insights from Kazakhstan's National Cybersecurity Center were examined to evaluate the domestic threat landscape. This helped identify key issues such as phishing attacks, malware incidents, and breaches of payment systems.

Second, an evaluation of the effectiveness of existing technical and organizational data protection measures was undertaken. The research reviewed practices such as multi-factor authentication, encryption protocols, and security auditing procedures in place within tourism organizations. Special emphasis was placed on assessing the functionality of Personal Data Information Systems (PDIS), with consideration of regulatory compliance, certification, and operational audits.

Third, a comparative legal analysis was carried out to benchmark Kazakhstan's data protection framework against leading international models, including the European Union's General Data Protection Regulation (GDPR), the U.S. California Consumer Privacy Act (CCPA), and Singapore's Personal Data Protection Act (PDPA). This comparative approach provided insight into the strengths and weaknesses of Kazakhstan's legal environment regarding cybersecurity in tourism.

Lastly, a survey of 112 professionals from Kazakhstan's tourism and aviation sectors (including employees from Air Astana, Fly Arystan, and Marriott hotels) was conducted to gather empirical data on current cybersecurity practices, awareness levels, and perceived risks. The results were used to construct visual analytics and a SWOT analysis, highlighting gaps and opportunities for improvement.

This integrative methodology ensured a reliable, evidence-based assessment and supported the formulation of practical and strategic cybersecurity recommendations tailored to the tourism industry.

Results and Discussion

Cyber threats today pose a serious risk to the security of travelers' data in the tourism sector. Phishing, malware, and payment data breaches are among the most common threats. Phishing is a fraudulent technique used by hackers who pose as trusted sources to obtain personal information such as credit card numbers or passwords. As the travel industry rebounds post-pandemic, it is increasingly targeted by automated threats, with the sector experiencing nearly 21% of all bot attack requests last year.

That's according to research by Imperva, a Thales company. In their 2024 Bad Bot Report, Imperva finds that bad bots accounted for 44.5% of the industry's web traffic in 2023 – a significant jump from 37.4% in 2022 (https://thehackernews.com). When attackers gain access to customers' payment details, it is classified as a payment data breach, which can lead to financial losses and erode customer trust in travel agencies (Karadayi-Usta, 2025).

The General Data Protection Regulation (GDPR) of the European Union sets strict guidelines for the processing of personal data, affecting businesses worldwide. The importance of cybersecurity is emphasized by real-world breaches in the tourism industry. For instance, in 2023, automated cyberattacks using bots to steal accounts and commit various types of fraud posed a new threat to the sector (Marengo & Pagano, 2024).

Such high-risk incidents lead to significant financial losses and damage a company's reputation. To improve cybersecurity in the tourism industry, it is essential to thoroughly analyze cyber threats, study relevant legislation, and examine actual data breach cases.

Evaluating the Effectiveness of Current Measures for Protecting Personal Data. Studies show that after implementing technical and organizational measures, it is crucial to assess their effectiveness–this includes conducting audits and recording outcomes. Developing a program and evaluation methodology that considers the characteristics of personal data information systems (PDIS) is an important step. Auditing and certifying PDIS allows us to determine whether the procedures in place comply with information security requirements. Therefore, the systematic evaluation and improvement of personal data protection protocols is a key component of ensuring information security in the tourism industry (Florido-Benítez, 2024).

Comparing International Cybersecurity Standards in the Travel and Tourism Sector. Using a comparative analysis approach, the study examined the legal foundations of cybersecurity in Kazakhstan and leading countries. The GDPR (European Union), CCPA (USA), and the Law on Personal Data and Their Protection (Kazakhstan) are legal frameworks governing the protection of personal data (Miller, 2024). By applying comparative analysis, we were able to identify the strengths and weaknesses of Kazakhstan's data protection laws and corporate standards (see Table 1).

Despite simple laws, Kazakhstan lags wealthy countries in the issue of cybersecurity in the travel and tourism sector. Strict regulations and heavy fines contribute to better data protection in Singapore and the EU. While the level of data protection in the USA varies depending on the state and company, large travel agencies actively utilize modern security methods.

Thanks to the widespread use of advanced technologies such as blockchain and biometrics, the likelihood of data theft is lower in the UAE and Singapore. Kazakhstan needs to tighten data storage regulations, implement stricter security measures, and raise awareness among travel agencies about online threats.

Table 1 – Comparison of cybersecurity criteria in tourism

Criteria	Kazakhstan	USA	UAE	European Union	Singapore
Law on data retention	Law of the Republic of Kazakhstan No. 94-V on Personal Data and Its Protection, dated May 21, 2013	Consumer Privacy Act (CCPA), FTC regulations	Data Protection Law (DPL, ADGM)	General Data Protection Regulation (GDPR)	Personal Data Protection Act (PDPA)
Penalties for breaking the law	A fine of up to 1600 Monthly Calculation Indexes (MCI) may be imposed	Fines up to $7,500	Fines of up to $28 million	Fines of up to 20 million euros	Fines of up to $1 million
Data retention requirements	The importance of protecting personal information is paramount.	Depending on each state, however, the requirements are limited.	It varies depending on the regions.	The data must be stored in the EU or countries with adequate protection.	Data must be stored in Singapore

Continuation of the table

Criteria	Kazakhstan	USA	UAE	European Union	Singapore
The level of entrepreneurs' awareness of legislation	Average: Many companies do not take the necessary measures	Average: Depends on state laws and business types	High: global standards are used in large companies	High: There are strict regulations and entrepreneurs are required to comply.	High: the state is actively implementing regulatory legal acts
Methods for protecting data	Only basic measures are used: password, antivirus	Encryption, payment data security	Biometrics, blockchain, advanced new technologies	Encryption, two-factor authentication, regular audits	Multi-factor authentication, access to data is always under control
Frequency of cyberattacks on travel companies	Above: Data leakage and phishing	Above: Personal information is often compromised in hotels	Low: very high level of technological protection	Moderate: The frequency of cyberattacks has decreased due to strict controls	Low: very strict rules and level of control
Training workers in cybersecurity	Not satisfactory because teaching is not mandatory	Optional	There are training programs at the national level.	Obliged to large companies	The state provides training for entrepreneurs
Implementing advanced security technologies.	Limited: only used in large companies	Rapidly developing in large companies	Uses advanced monitoring, including blockchain and Artificial Intelligence	Uses Blockchain and Artificial Intelligence monitoring	Public and private companies are using Artificial Intelligence and analytics
The level of trust in the protection of tourists' data	Low: many fraudulent incidents occur	Average: varies depending on the company	High: Strict security measures are in place	Above: Tourists gain confidence thanks to strict laws	High: users are confident that their data is secure

Note: Compiled by the authors based on the literary sources (Arcuri et al., 2020; del Mar Alonso-Almeida et al., 2024; Ghaderi, Beal, Hall, et al., 2024; Tariq, 2024).

Surveys with tourism and IT experts. A survey was conducted on the cybersecurity practices used by employees in Kazakhstan's hotels, travel agencies, and the aviation industry. The survey included 112 respondents, including employees from Air Astana, Fly Arystan Airlines, and the Marriott hotel chain.

According to the survey, 14.3% of participants indicated that the protection measures are insufficient. In comparison, 42.9% of respondents directly state that information security issues are not a priority, which highlights the significant risks associated with the disclosure of travelers' data (Figure 1).

To achieve the purpose of the survey, respondents were asked about the methods used in their companies to protect clients' personal information, and they were given several options to choose from. According to the responses, most companies use basic data protection methods.

42.9% of respondents reported that their companies use data encryption methods, while 85.7% stated that multi-factor authentication is implemented in their companies. Additionally, 57.1% of respondents indicated that their companies provide cybersecurity training for employees, and 71.4% reported that employees do not have access to customers' personal information (Figure 2).

Respondents' responses to the question of how often their company conducts training or briefings on safety issues are shown in Figure 3.

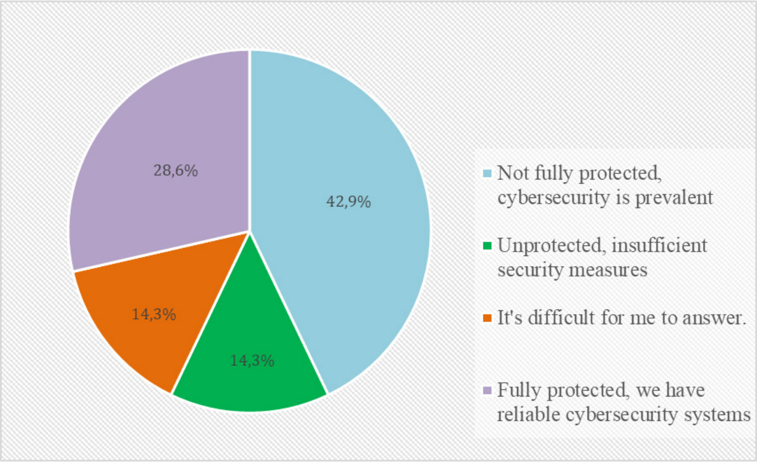

Figure 1 – Diagrammatic analysis of how protected tourism companies are from cyber threats
Note: Compiled by the authors based on survey responses

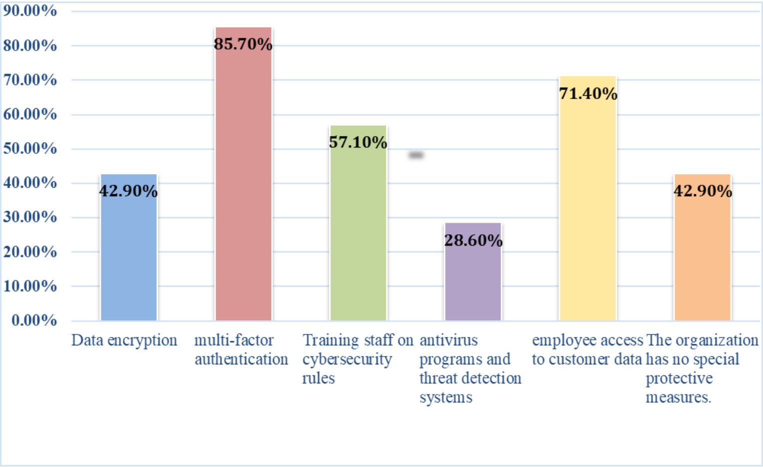

Figure 2 – Methods of protecting clients' data in tourism companies
Note: Compiled by the authors based on survey responses

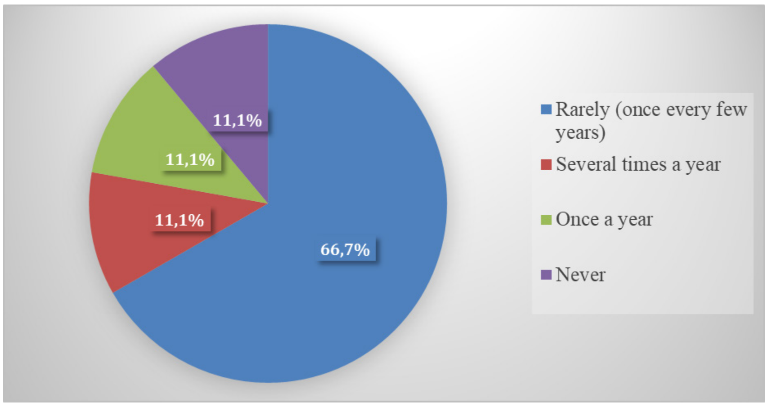

Figure 3 – Responses to the company's conduct training or briefings on cybersecurity issues
Note: Compiled by the authors based on survey responses

The next question of the survey asked respondents how often training and briefings on cybersecurity issues are conducted in their company. 66.7% of respondents reported that they are held rarely, while 11.1% indicated that they are held once a year. Additionally, another 11.1% of respondents stated that training sessions are held several times a year, while the remaining 11.1% reported that such events have never taken place (Figure 3).

Respondents' responses to the question of which cyber threats pose the greatest threat to their company are shown in Figure 4.

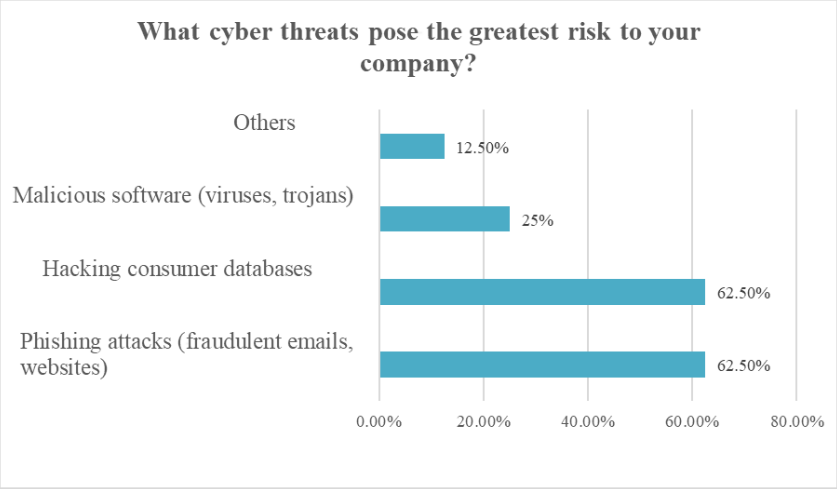

Figure 4 – Responses to cyber threats pose the greatest risk to the company
Note: Compiled by the authors based on survey responses

The survey asked what cyber threats could pose to tourism companies. Respondents were given several options to choose from. According to the results, 62.5% indicated that phishing attacks, such as fraudulent emails and websites, pose a high risk, while the next 62.5% highlighted the danger of customer database breaches. Additionally, 25% of respondents pointed to the presence of malicious software viruses, and 12.5% selected other cyber threats (Figure 4).

Respondents' responses to the question whether they think their company should increase investment in cybersecurity are shown in Figure 5.

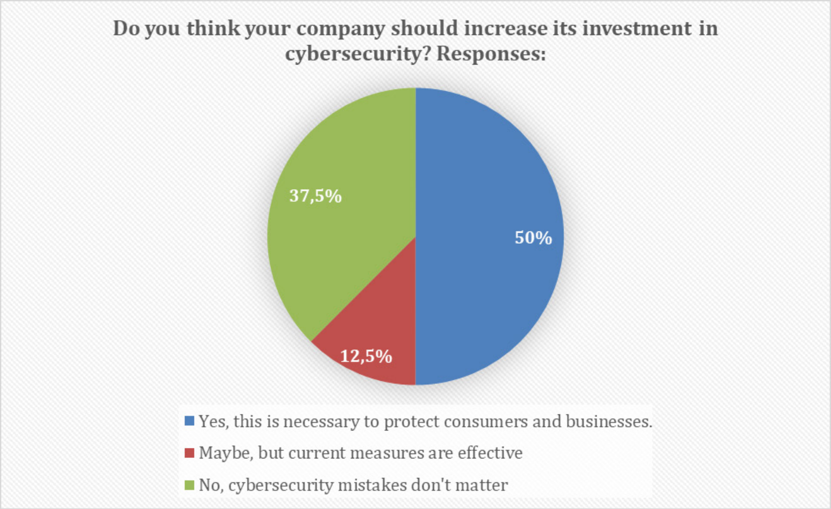

Figure 5 – Responses to the company's increase in investment in cybersecurity
Note: Compiled by the authors based on survey responses

To conclude the survey, respondents were asked about the importance of increasing investment to strengthen cybersecurity in their tourism companies. 50% supported the idea, stating that it is necessary to protect customers and businesses. Meanwhile, 37.5% considered increasing investment unnecessary, as they did not see cybersecurity threats as important. 12.5% believed that the current cybersecurity measures were effective.

Considering the increasing threat of cyberattacks in Kazakhstan's tourism sector, comprehensive measures must be taken to protect tourists' personal data and improve cybersecurity. Through the analysis of collected data, we identified current vulnerabilities in protecting visitor information and provided recommendations to enhance cybersecurity in Kazakhstan.

- Creating and implementing a security policy. Tourism industry organizations should develop and implement data protection policies and guidelines that align with global standards. The Kazakhstan Data Protection Association is actively working on developing such standards, which could serve as a model for other organizations. For example, tourism companies should develop internal information security policies, including rules for handling clients' personal data, and formalize them. To prevent unauthorized access to personal data, multi-factor authentication (MFA) should be implemented. The access level for each employee should be defined and enforced. For example, booking managers can view customer data but should not have access to payment details.

- Regular vulnerability assessment and audits. Tourism companies should use specialized tools such as Nessus or OpenVAS to scan for any weaknesses in their IT infrastructure automatically. These tools can immediately detect threats when cybersecurity levels are low or when issues arise and alert IT professionals. In turn, the professionals can address the weaknesses. Additionally, independent experts should be invited to conduct annual cybersecurity audits. This means supporting government checks to assess the cybersecurity level in tourism companies and obtaining feedback from experts.

Based on the research, a special SWOT analysis of the current state of cybersecurity in Kazakhstan's tourism sector was conducted (Table 2).

Table 2 – SWOT Analysis of Cybersecurity in the Tourism Sector of Kazakhstan

S (strengths)	W (weaknesses)
− The development of digital and online service technologies in tourism; − Measures taken by the government to strengthen cybersecurity; − Access to international best practices has resulted in the adoption of high-standard data protection techniques; − The growth of domestic tourism has led to a reduction in the use of foreign platforms; − An increase in the number of tourism enterprises considering the importance of personal data protection.	− The weak level of cybersecurity in small and medium-sized businesses; − The low level of digital literacy among employees; − The shortage of specialists in the field of cybersecurity; − The weakness of internal security systems leading to the potential theft of personal data; − The lack of transparency in data storage and processing in tourism companies.
O (opportunities)	T (threats)
− The implementation of new technologies for data storage and protection (Artificial Intelligence, Blockchain); − Strengthening the security level of local booking and payment platforms; − Government programs to support digital transformation; − Training and development of specialists in the field of cybersecurit	− The increasing frequency of cyberattacks on tourism services and platforms; − The theft of personal data leading to a loss of trust from tourists; − The high costs associated with ensuring compliance with cybersecurity standards; − The growth of fraud schemes related to tourism services; − The use of outdated booking and payment systems.
Note– (Nussarova A., & Jaksylykov S., 2020; Data Protection Regulations, URL 1: 2021; Ovchinnikov Yu., & Ravkin R., 2021; Kobets P., 2020) compiled by the author based on research conducted	

*Note: Compiled by the authors based on the conducted researches (Hallinan et al., 2021; Кобец, 2020; Нусарова, 2020; Овчинников & Равкин, 2021)***.**

- Employee training. Tourism companies should train their employees on cybersecurity, including teaching them how to recognize phishing attacks. A test should be conducted to assess the knowledge acquired by employees. For example, sending fake phishing emails and monitoring employees' responses. An emergency response manual should be developed for situations where customer data is compromised or when a cyberattack occurs. The cybersecurity guidelines from Kazakhstan's Ministry of Digital Development, Innovations, and Aerospace Industry can be used for employee training.

- Using modern security technologies. Information security can be significantly improved through the use of modern technologies such as data encryption, multi-factor authentication, monitoring, and intrusion detection systems. To implement security technologies, DDoS protection systems like Cloudflare or Imperva can be introduced. Additionally, advanced antivirus protection and intrusion detection/prevention systems (IDS/IPS) would be an effective solution. To protect customers' personal data, backups can be created and encrypted.

- Cooperation with government agencies. Collaboration with government organizations such as the Information Security Committee of the Ministry of Digital Development, Innovations, and Aerospace Industry of the Republic of Kazakhstan, as well as with professional associations, provides an opportunity for knowledge exchange and access to up-to-date information on emerging threats and defense strategies.

- The viable way to improve cybersecurity in Kazakhstan's tourism sector is through the use of artificial intelligence (AI). AI technologies enable real-time analysis of network traffic, detection of anomalies, and prevention of cyberattacks such as phishing and payment data breaches. Integrating AI into both public and private sectors can help improve information security and facilitate a quick response to incidents. Therefore, integrating AI into cybersecurity measures is an important first step to ensuring reliable data protection in Kazakhstan's tourism industry.

The findings of this study confirm that cybersecurity has become a critical challenge for the modern tourism industry. As digital technologies become increasingly embedded in tourism services, particularly in online booking platforms, electronic payment systems, and mobile applications, cyber threats grow in complexity and frequency. The results of this research show that tourism companies are highly vulnerable to phishing schemes, data breaches, and malware attacks, which can lead to the unauthorized disclosure of travelers' personal and financial information.

One of the key insights from the survey conducted in Kazakhstan is the lack of cybersecurity preparedness, especially among small and medium-sized enterprises. While large companies like Air Astana and Marriott have introduced encryption, multi-factor authentication, and employee training programs, the broader tourism ecosystem continues to struggle with basic security implementation. This creates a fragmented security environment that compromises consumer trust and increases systemic risk.

Comparative analysis with international frameworks such as the GDPR (EU), CCPA (USA), and PDPA (Singapore) highlights the gap between Kazakhstan and more cyber-resilient jurisdictions. In these leading countries, strict penalties, centralized regulatory oversight, and frequent audits compel tourism companies to adopt high security standards. Kazakhstan's current legal framework lacks the specificity and enforcement mechanisms necessary to ensure sector-wide compliance.

Furthermore, the study illustrates that technical solutions alone are not sufficient. Organizational awareness, employee training, and a proactive cybersecurity culture are essential to protecting sensitive traveller data. Encouragingly, government-backed programs such as "Digital Kazakhstan" offer a platform for broader adoption of secure digital practices, but more sector-specific guidance and support are needed.

Overall, this discussion emphasizes that achieving robust cybersecurity in tourism requires a multilayered approach: integrating advanced technologies, improving legal enforcement, and fostering a culture of digital responsibility. This will not only protect travellers but also enhance the competitiveness and sustainability of the tourism industry.

Conclusion

The rapid digitalization of the tourism industry has introduced significant advantages in terms of efficiency and service delivery. However, it has also exposed the sector to a growing number of cyber threats, ranging from phishing schemes and malware to data breaches and identity theft. This study has demonstrated that the tourism sector, both globally and in Kazakhstan, remains highly vulnerable to cyberattacks due to increasing reliance on digital platforms for bookings, payments, and customer service.

The research identified key cybersecurity risks affecting tourism companies and analyzed their underlying causes, including insufficient investment in protective infrastructure, lack of staff training, outdated IT systems, and weak legal enforcement. Through comparative analysis, Kazakhstan's data protection framework was found to be less robust than those in countries such as the European Union, the United States, and Singapore, where strict cybersecurity regulations and advanced technologies are actively enforced.

Survey results from tourism and aviation sector employees in Kazakhstan revealed that while some large companies are adopting multi-factor authentication and data encryption, a majority of small and medium-sized enterprises continue to rely on basic security measures, if any. This gap highlights the urgent need for industry-wide improvements in cybersecurity culture and practice.

To mitigate existing vulnerabilities, the study recommends the adoption of modern security technologies, including artificial intelligence, blockchain, and real-time threat detection systems. Furthermore, regular cybersecurity audits, clear data access policies, mandatory employee training, and alignment with international regulatory standards are essential to safeguard personal information in tourism operations.

Research findings also indicate that many tourism organizations do not pay sufficient attention to cybersecurity, often limiting themselves to only basic security measures. This, in turn, can lead to the loss or unauthorized access to users' personal data and financial information. Such incidents not only result in financial losses but also damage the company's reputation and undermine consumer trust.

In this context, ensuring cybersecurity in the tourism sector requires comprehensive and coordinated actions. These should encompass a wide range of measures, from regulatory and legal frameworks at the national level to the development of information security strategies within individual organizations and the training of qualified specialists. Moreover, fostering a culture of security, implementing advanced protection technologies (such as blockchain, artificial intelligence, and encryption), and engaging in international knowledge exchange play a crucial role.

Ultimately, improving cybersecurity in the tourism industry is not only about protecting data but also about maintaining the trust and confidence of travelers. A well-structured cybersecurity strategy will enhance service quality, reduce legal and financial risks, and support the sustainable digital transformation of the tourism sector.

Overall, the research highlights the urgent need to implement concrete steps and recommendations to enhance digital security in Kazakhstan's tourism industry. In the long term, systematic efforts in this direction are expected to improve the reliability and competitiveness of tourism services.

Conflict of Interest Statement

The authors declare no potential conflicts of interest regarding the research, authorship, or publication of this article.

Acknowledgments

The author(s) received no financial support for the research, authorship, and/or publication of this article. We are grateful to our institutions. Also, many thanks to the anonymous reviewers for their helpful comments and guidance. Lastly, thank you to the survey participants who provided valuable insights.

References

Arcuri, M. C., Gai, L., Ielasi, F., & Ventisette, E. (2020). Cyber attacks on hospitality sector: Stock market reaction. *Journal of Hospitality and Tourism Technology*, *11*(2), 277-290.

Baik, J. S. (2020). Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA). *Telematics and Informatics*, *52*.

del Mar Alonso-Almeida, M., & Giglio, C. (2024). Cybersecurity in tourism and hospitality management research: current issues, trends, and an agenda for future research. *Cuadernos de turismo*(53), 243-260.

del Mar Alonso-Almeida, M., Giglio, C., & Iazzolino, G. (2024). A cross-country analysis of decision-making factors influencing tourists' shift towards circular destinations in EU-27. *Socio-Economic Planning Sciences*, *94*, 101955.

Florido-Benítez, L. (2024). The cybersecurity applied by online travel agencies and hotels to protect users' private data in smart cities. *Smart Cities*, *7*(1), 475-495.

Florido-Benítez, L. (2025). The role of cybersecurity as a preventive measure in digital tourism and travel: a systematic literature review. *Discover Computing*, *28*(1), 28.

Ghaderi, Z., Beal, L., Hall, C. M., Zaman, M., Ahmad Rather, R., & Mat Som, A. P. (2024). Cybersecurity and smart tourist destinations resilience. *Tourism Recreation Research*, 1-17.

Ghaderi, Z., Beal, L., & Houanti, L. (2024). Cybersecurity threats in tourism and hospitality: perspectives from tourists engaging with sharing economy services. *Current Issues in Tourism*, 1-16.

Hallinan, D., De Hert, P., & Leenes, R. (2021). Data Protection and Privacy.

https://thehackernews.com. Automated Threats Pose Increasing Risk to the Travel Industry. Jul 18, 2024: https://thehackernews.com/2024/07/automated-threats-pose-increasing-risk.html.

Karadayi-Usta, S. (2025). Sustainable medical tourism service network with a stakeholder perspective. *Current Issues in Tourism*, *28*(2), 321-340.

Marengo, A., & Pagano, A. (2024). Machine learning for cybersecurity for detecting and preventing cyber attacks. *Machine Intelligence Research*, *18*(1), 672-689.

Miller, K. (2024). Cyber Security Threats in Tourism and Hospitality. URL: https://trainingcamp.com/cyber-security-threats-in-tourism-and-hospitality/ (Қарау уақыты: 04.02.2024).

Paraskevas, A. (2022). Cybersecurity in travel and tourism: a risk-based approach. In *Handbook of e-Tourism* (pp. 1605-1628). Springer.

Perlroth, N., Tsang, A., & Satariano, A. (2018). Marriott hacking exposes data of up to 500 million guests. *The New York Times*, *30*.

Roy, P., Chandrasekaran, J., Lanus, E., Freeman, L., & Werner, J. (2023). A Survey of Data Security: Practices from Cybersecurity and Challenges of Machine Learning. *arXiv preprint arXiv:2310.04513*.

Syzdykova, D., Yuldasheva, N., Abdramanova, G., Kose, Z. K., & Isaeva, A. (2024). Проблемы и перспективы развития туристского бизнеса в Казахстане. *Bulletin of the Karaganda university Economy series*, *11329*(1), 193-203.

Tariq, M. U. (2024). Cybersecurity risk assessment models and theories in the travel and tourism industry. In *Corporate Cybersecurity in the Aviation, Tourism, and Hospitality Sector* (pp. 1-17). IGI Global.

Thealla, P., Nadda, V., Dadwal, S., Oztosun, L., & Cantafio, G. (2024). *Corporate cybersecurity in the aviation, tourism, and hospitality sector*. IGI Global.

Williamson, J., & Curran, K. (2021). Best practice in multi-factor authentication. *Semiconductor Science and Information Devices*, *3*(1).

Zishan, M., & Russell, S. (2024). Data Privacy and Security in E-commerce: Utilizing Blockchain and Multi-Factor Authentication to Safeguard Transactions. *ResearchGate, August 2024, DOI: http://dx. doi. org/10.13140/RG. 2.2*, *16554*.

Кобец, П. Н. (2020). Обеспечение безопасности туристической индустрии-одна из важнейших составляющих ее эффективного развития. *Диалог*(2 (16)), 20-29.

Мосунова, Н. (2024). Air Astana подтвердила безопасность персональных данных пассажиров [Электронды ресурс] // Казинформ. URL: https://www.inform.kz/ru/air-astana-podtverdila-bezopasnost-personalnih-dannih-passazhirov-0adfe6 (Қарау уақыты: 01.02.2024).

Нусарова, А., & Джаксылыков, С. (2020). *Защита персональных данных в Казахстане: статус, риски и возможности: https://www.soros.kz/wp-content/uploads/2020/04/Personal_data_report.pdf*.

Овчинников, Ю. Д., & Равкин, Р. Д. (2021). Проблемы технократичности и безопасности в сфере туризма. *Наука-2020*(4 (49)), 127-132.

References

Arcuri, M. C., Gai, L., Ielasi, F., & Ventisette, E. (2020). Cyber attacks on hospitality sector: Stock market reaction. Journal of Hospitality and Tourism Technology, 11(2), 277-290.

Baik, J. S. (2020). Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA). Telematics and Informatics, 52.

del Mar Alonso-Almeida, M., & Giglio, C. (2024). Cybersecurity in tourism and hospitality management research: current issues, trends, and an agenda for future research. Cuadernos de turismo(53), 243-260.

del Mar Alonso-Almeida, M., Giglio, C., & Iazzolino, G. (2024). A cross-country analysis of decision-making factors influencing tourists' shift towards circular destinations in EU-27. Socio-Economic Planning Sciences, 94, 101955.

Florido-Benítez, L. (2024). The cybersecurity applied by online travel agencies and hotels to protect users' private data in smart cities. Smart Cities, 7(1), 475-495.

Florido-Benítez, L. (2025). The role of cybersecurity as a preventive measure in digital tourism and travel: a systematic literature review. Discover Computing, 28(1), 28.

Ghaderi, Z., Beal, L., Hall, C. M., Zaman, M., Ahmad Rather, R., & Mat Som, A. P. (2024). Cybersecurity and smart tourist destinations resilience. Tourism Recreation Research, 1-17.

Ghaderi, Z., Beal, L., & Houanti, L. (2024). Cybersecurity threats in tourism and hospitality: perspectives from tourists engaging with sharing economy services. Current Issues in Tourism, 1-16.

Hallinan, D., De Hert, P., & Leenes, R. (2021). Data Protection and Privacy.

https://thehackernews.com. Automated Threats Pose Increasing Risk to the Travel Industry. Jul 18, 2024: https://thehackernews.com/2024/07/automated-threats-pose-increasing-risk.html.

Karadayi-Usta, S. (2025). Sustainable medical tourism service network with a stakeholder perspective. Current Issues in Tourism, 28(2), 321-340.

Marengo, A., & Pagano, A. (2024). Machine learning for cybersecurity for detecting and preventing cyber attacks. Machine Intelligence Research, 18(1), 672-689.

Miller, K. (2024). Cyber Security Threats in Tourism and Hospitality. URL: https://trainingcamp.com/cyber-security-threats-in-tourism-and-hospitality/ (Қарау уақыты: 04.02.2024).

Paraskevas, A. (2022). Cybersecurity in travel and tourism: a risk-based approach. In Handbook of e-Tourism (pp. 1605-1628). Springer.

Perlroth, N., Tsang, A., & Satariano, A. (2018). Marriott hacking exposes data of up to 500 million guests. The New York Times, 30.

Roy, P., Chandrasekaran, J., Lanus, E., Freeman, L., & Werner, J. (2023). A Survey of Data Security: Practices from Cybersecurity and Challenges of Machine Learning. arXiv preprint arXiv:2310.04513.

Syzdykova, D., Yuldasheva, N., Abdramanova, G., Kose, Z. K., & Isaeva, A. (2024). Problems and Prospects for the Development of the Tourism Business in Kazakhstan. Bulletin of the Karaganda university Economy series, 11329(1), 193-203. (In Russian)

Tariq, M. U. (2024). Cybersecurity risk assessment models and theories in the travel and tourism industry. In Corporate Cybersecurity in the Aviation, Tourism, and Hospitality Sector (pp. 1-17). IGI Global.

Thealla, P., Nadda, V., Dadwal, S., Oztosun, L., & Cantafio, G. (2024). Corporate cybersecurity in the aviation, tourism, and hospitality sector. IGI Global.

Williamson, J., & Curran, K. (2021). Best practice in multi-factor authentication. Semiconductor Science and Information Devices, 3(1).

Zishan, M., & Russell, S. (2024). Data Privacy and Security in E-commerce: Utilizing Blockchain and Multi-Factor Authentication to Safeguard Transactions. ResearchGate, August 2024, DOI: http://dx. doi. org/10.13140/RG. 2.2, 16554.

Kobets, P. N. (2020). Ensuring the security of the tourism industry as one of the key components of its effective development. Dialog, 2(16), 20–29. (In Russian)

Mosunova, N. (2024). Air Astana confirmed the security of passengers' personal data [Electronic resource]. Kazinform. https://www.inform.kz/ru/air-astana-podtverdila-bezopasnost-personalnih-dannih-passazhirov-0adfe6 (Retrieved February 1, 2024). (In Russian)

Nusarova, A., & Dzhaksylykov, S. (2020). Personal data protection in Kazakhstan: Status, risks, and opportunities. https://www.soros.kz/wp-content/uploads/2020/04/Personal_data_report.pdf. (In Russian)

Ovchinnikov, Y. D., & Ravkin, R. D. (2021). Problems of technocracy and security in the field of tourism. Science-2020, 4(49), 127–132. (In Russian)

***Information about authors*:**

Zhannat Aliyeva – Candidate of Geographical Sciences, Associate Professor, Al-Farabi Kazakh National University (Almaty, Kazakhstan, e-mail: aliyeva.zhannat@kaznu.kz);

Zhanel Baden – Bachelor's Degree Student majoring in Tourism, Al-Farabi Kazakh National University (Almaty, Kazakhstan, e-mail: zhanel.baden@gmail.com);

Imanaly Akbar (corresponding author) – PhD, Acting Associate Professor, Al-Farabi Kazakh National University (Almaty, Kazakhstan, e-mail: akbar.imanaly@gmail.com);

Zabira Myrzaliyeva – Candidate of Geographical Sciences, Senior Lecturer, South Kazakhstan Pedagogical University named after Uzbekali Zhanibekov (Shymkent, Kazakhstan, e-mail: zabira2011@mail.ru);

Madeleine Udahogora – PhD, Project Manager, Rwanda Rural Rehabilitation Initiative NGO (Kigali, Rwanda, e-mail: umadeleine@rwarri.com).

Авторлар туралы мәлімет:

Жаннат Алиева Нарикбаевна – география ғылымдарының кандидаты, доцент, әл-Фараби атындағы ҚазҰУ (Алматы, Қазақстан, e-mail: aliyeva.zhannat@kaznu.kz);

Жәнел Бәден Сырымқызы – туризм мамандығы бойынша бакалавриат студенті, әл-Фараби атындағы ҚазҰУ (Алматы, Қазақстан, e-mail: zhanel.baden@gmail.com);

Иманалы Акбар (корреспонденттік автор) – PhD докторы, доцент м. а., әл-Фараби атындағы ҚазҰУ (Алматы, Қазақстан, e-mail: akbar.imanaly@gmail.com);

Забира Мырзалиева Қазыбекқызы – география ғылымдарының кандидаты, аға оқытушы, Өзбекәлі Жәнібеков атындағы Оңтүстік Қазақстан педагогикалық университеті (Шымкент, Қазақстан, e-mail: zabira2011@mail.ru);

Мадлен Удахогора – PhD, жоба жетекшісі, Руанда ауылдық жерлерін қалпына келтіру бастамасы ҮЕҰ (Кигали, Руанда, e-mail: umadeleine@rwarri.com).

Сведения об авторах:

Алиева Жаннат Нарикбаевна – кандидат географических наук, доцент Казахского национального университета имени аль-Фараби (Алматы, Казахстан, e-mail: aliyeva.zhannat@kaznu.kz);

Баден Жанель Сырымовна – студентка бакалавриата по специальности «Туризм», Казахский национальный университет имени аль-Фараби (Алматы, Казахстан, e-mail: zhanel.baden@gmail.com);

Акбар Иманалы (ответственный автор) – доктор философии, и. о. доцента Казахского национального университета имени аль-Фараби (Алматы, Казахстан, e-mail: akbar.imanaly@gmail.com);

Мырзалиева Забира Казыбеккызы – кандидат географических наук, старший преподаватель, Южно-Казахстанский педагогический университет им. Өзбекәлі Жәнібеков (Шымкент, Казахстан, e-mail: zabira2011@mail.ru);

Мадлен Удахогора – доктор философии, руководитель проекта, НПО «Инициатива по восстановлению сельских районов Руанды» (Кигали, Руанда, e-mail: umadeleine@rwarri.com).

Received: June 1, 2025
Accepted: October 20, 2025