UDC 343.98:65.011
DOI: 10.32518/sals2.2025.285

Criminal law support for information security: Issues of theory and practice

Sergey Salishev
Postgraduate Student
Jusup Balasagyn Kyrgyz National University
720033, 547 Frunze Str., Bishkek, Kyrgyz Republic
https://orcid.org/0009-0008-5759-589

Baktygul Kanybekova
PhD in Law, Associate Professor
National Academy of Sciences of the Kyrgyz Republic
720071, 265-A Chui Ave., Bishkek, Kyrgyz Republic
https://orcid.org/0009-0006-3741-601X

Almagul Kokoeva
Doctor of Law, Professor
Kyrgyz-Uzbek International University named after B. Sydykov
720082, 27 G. Aitiev Str., Osh, Kyrgyz Republic
https://orcid.org/0009-0006-1893-8365

Chynara Botoeva
Doctor of Law, Acting Professor
Academy of Public Administration under the President of the Kyrgyz Republic named after Zh. Abdrakhmanov
720040, 237 Panfilov Str., Bishkek, Kyrgyz Republic
https://orcid.org/0009-0006-4075-8192

Bakyt Kakeshov*
PhD in Law, Associate Professor
Jusup Balasagyn Kyrgyz National University
720033, 547 Frunze Str., Bishkek, Kyrgyz Republic
https://orcid.org/0000-0003-1570-1072

Abstract. The study analysed the criminal law mechanism for ensuring information security as one of the key elements of the national security of the State. The study aimed to conduct research on criminal law provision of information security in the context of modern challenges of the digital environment and to identify the areas for improvement of criminal law for effective response to information threats. It was done by looking at national and foreign laws, court cases, and stats on cybercrime, as well as using systematic, comparative, and formal legal analysis. Key threats to information security that have become widespread in Kyrgyzstan and abroad were identified, including unauthorised interference in information systems, illegal collection of personal data and dissemination of harmful content. A comparative legal analysis of the criminal legislation of Germany, France, the USA, Poland and Kyrgyzstan was conducted to identify effective approaches to criminalisation and punishment of the relevant offences. The study established that the model of criminal law protection needs to be updated with due regard to international experience in terms of distinguishing cybersecurity offences and improving the qualifying features. It has been established that the current criminal legislation

Suggested Citation

Article's History: Received: 10.03.2025 Revised: 25.05.2025 Accepted: 25.06.2025

Salishev, S., Kanybekova, B., Kokoeva, A., Botoeva, Ch., & Kakeshov, B. (2025). Criminal law support for information security: Issues of theory and practice. *Social & Legal Studios*, 8(2), 285-296. doi: 10.32518/sals2.2025.285.

*Corresponding author

of Kyrgyzstan needs further adaptation to modern challenges in the field of digital technologies in order to improve the classification of acts related to interference in information systems and differentiate liability. The practical significance of the results is determined by the formulation of proposals for improving legislation and the application of criminal law means to improve the effectiveness of information security protection at both the national and international levels

Keywords: information security; national security; cybercrime; information threats; media literacy; international cooperation

Introduction

In a rapidly digitising society, information security is becoming a fundamental factor in the stable functioning of the state, business and personal sphere of citizens. The economic, political and social security of the country, and thus its national security in general, largely depends on the effectiveness of information space protection. In Kyrgyzstan, as in the United States, France, Germany and Poland, the number of cybercrimes, personal data leaks, and interference with government systems is growing, which creates an objective need to improve criminal law mechanisms for responding to these challenges. However, existing criminal legal systems do not always meet the rapid development of digital threats. Criminal law, as a protection of the most important social values, does not always have adequate means to respond to new forms of information crime (Mentukh, & Shevchuk, 2023). The research relevance also is determined by the rapid development of information technology and the simultaneous increase in the number and complexity of information security crimes, which the current criminal legislation of many countries, including Kyrgyzstan, the United States, France, Germany and Poland, is not always able to effectively prevent and properly prosecute. The main problem is the fragmentation of legal regulation, unclear terminology, lack of a unified approach to defining the elements of information crimes, as well as difficulties in law enforcement related to the transnational nature of many information offences.

This problem has been addressed from various angles in scientific literature. For example, B.D. Kakeshov (2023) analysed the political and legal aspects of liability for information security offences in the context of national security in Kyrgyzstan, with a particular focus on the relationship between criminal and administrative liability. According to the author, Kyrgyzstan could implement comprehensive cybersecurity laws and strengthen institutional capacities, while also fostering public-private partnerships and investing in advanced technologies to enhance its defense against cyber threats. Additionally, raising public awareness and engaging in international cooperation can further bolster the nation's cybersecurity framework. M. Jurgilewicz and O. Jurgilewicz (2019) analysed issues of information security management and its criminal law protection in the context of Polish practice. The authors emphasised the need to improve legislative norms and enhance the qualifications of law enforcement officials to respond effectively to information threats. The importance of interagency cooperation and the development of a unified security strategy is noted. Theoretical approaches, according to the researchers, should be backed up by practical measures, including prevention and high-quality investigation.

The study by T.L. Chapman and S. Chaudoin (2020) highlighted the perception of international criminal institutions by the population in developing countries, demonstrating the link between trust in the justice system and the effectiveness of legal regulation in the field of security. The main patterns of use of digital assets in illegal activities, as identified by C. Nolasco Braaten and M.S. Vaughn (2021), include their use in money laundering, fraud, ransomware attacks, and illicit transactions on the dark web. These activities exploit the anonymity and decentralised nature of cryptocurrencies to facilitate various forms of cybercrime. C.J. Najdowski and M.C. Stevenson (2022) emphasise the need to reform the criminal law system to combat systemic inequality, which is also relevant to the field of information security, where unequal access to digital resources creates additional challenges. R. Atadjanov (2022) discussed the absence of crimes against humanity in the criminal legislation of Central Asian states, including Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan. The author provides an overview of the current status of these crimes under international law and analyses the domestic legislation of these countries. The Article studied strengthening the current Criminal Codes by incorporating well-formulated dispositions on crimes against humanity, considering the peculiarities of national legal systems. E. Marat and G. Botoeva (2022) examined the connections between illegal drug trafficking, violence, and corruption in Central Asia. The authors argue that drug trafficking in the region is highly organised, involving major criminal and state actors, with periodic changes among the involved parties. The analysis of violence and policing dynamics shows how patterns of organised crime are influenced by state effectiveness, state protection of trafficking, and competition among traffickers. Criminal violence is widespread, particularly in urban areas, but Central Asian states have shown capabilities in intercepting and preventing illicit activities (Dzyana & Dzyanyy, 2023). The authors recommend that the international community should focus on increasing the costs of corruption and rewarding good practices by political incumbents and their non-state collaborators.

The study aimed to form a holistic view of the criminal law provision of information security, to identify theoretical gaps and practical problems in law enforcement, and to develop substantiated proposals for improving the relevant legislation. To achieve this goal, the research analysed the concept and structure of information security in the criminal law context, studying the composition and specifics of crimes in this area, identifying the peculiarities of their qualification and proof, as well as researching national and international practices of criminal prosecution.

Materials and methods

In the first stage, an analysis of regulatory and legal acts governing cybercrime and information security in various countries was conducted, such as Law of the Kyrgyz Republic No. 121 "On Cybersecurity of the Kyrgyz Republic" (2024), Criminal Code of the Kyrgyz Republic (1997), Computer Fraud and Abuse Act (1986), Penal Code of France (1994), Criminal Code of Germany (1998), Criminal Code of the

Republic of Poland (1997), Act of the Republic of Poland "On the National Cybersecurity System" (2018); case law in such cases as Mckinnon v. Government of The United States of America and Another (2007), United States v. Andrew Auernheimer (2014), United States v. Swartz (2013), Van Buren v. United States (2021). For the study, normative legal acts and judicial practice of Kyrgyzstan, the United States, France, Germany and Poland were selected, as these countries demonstrate different models of criminal law regulation in the field of information security. Kyrgyzstan is an example of a post-Soviet jurisdiction that is in the process of actively forming a regulatory framework for cybersecurity.

The empirical part of the study included an online survey of 50 law enforcement officers from Kyrgyzstan and Poland. All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and national research committee and with the ICC/ESOMAR International Code on Market, Opinion and Social Research and Data Analytics (2016). The survey covered their experience in combating cybercrime, the level of training of specialists, and technical support. Respondents were selected from among employees working in cybercrime units. The total sample consisted of 50 people, 25 respondents from each country, which enabled a basic comparative analysis. The criteria for inclusion in the study were: age between 25 and 55, at least three years of practical experience in the field of cybercrime and confirmed voluntary consent. Exclusion criteria included lack of relevant experience, incomplete questionnaire completion, or withdrawal of consent. All respondents were informed of the voluntary nature of participation and of the possibility to withdraw at any stage without explanation. The survey was conducted anonymously online in March 2025. The questionnaire consisted of 20 fixed questions covering key aspects of law enforcement, professional training, technical support and legislative challenges in the field of information security. Respondents were selected from among employees working in cybercrime units. Standard data processing methods, such as calculating percentages and comparing different countries, were used for statistical analysis of the survey results. This identified the main problems in the application of criminal law and areas for improvement. Standard methods such as descriptive statistics, comparisons between groups and correlation analysis were used to process the statistical data in the study. Excel software was used for this purpose. Given the sensitivity of the subject matter, all surveys were anonymous. Respondents were informed in advance of the voluntary nature of their participation and that no personal or professional data would be collected, stored or transferred to third parties. The confidentiality of the results was guaranteed at all stages of the study, and responses were processed exclusively in an anonymised form following the ethical principles of social research.

Results

The concept of information security covers a set of social relations related to the protection of information resources from internal and external threats. In the modern legal framework, ensuring information security is considered one of the priority areas of state policy, as a breach of information security can lead to significant consequences for the economy, public administration, human rights and social stability (Zwilling *et al.*, 2020). In Kyrgyzstan, the definition of information security is enshrined in the Law of the Kyrgyz Republic No. 121 "On Cybersecurity of the Kyrgyz Republic" (2024), where it is interpreted as a state of information security that ensures its safety, integrity, confidentiality and availability. The law also provides for the classification of threats and liability for information offences. For instance, the Criminal Code of the Kyrgyz Republic (1997) contains several articles directly related to cybercrime, including Articles 211 (Unauthorised access to computer information) and 212 (Violation of the rules for the operation of computers, systems and networks), which provide criminal law protection of digital objects.

In the United States, information security is regulated primarily at the federal level through a series of laws, the most important of which is the Computer Fraud and Abuse Act (1986), which was passed in 1986 but has been updated many times. For instance, Section §1030 of this act provides for liability for intentional unauthorised access to a computer with the intent to obtain information from the federal government, financial institutions, or computers used in interstate or international commerce. One practical example is the case of United States v. Swartz (2013), where a well-known activist was accused of downloading millions of scientific articles from the closed JSTOR database without permission. In France, the concept of information security is defined through the prism of the protection of information systems and personal data. Article 323-1 of the Penal Code of France (1994) qualifies unauthorised access to automated data processing as a crime. If such access results in the destruction or modification of data, increased liability is provided. The law also protects the infrastructure of critical information systems (CIIP), for example in the energy and telecommunications sectors. In 2009, France established the Cybersecurity Agency (ANSSI), which coordinates digital security policy (D'Elia, 2018). Germany has one of the most developed legal mechanisms for combating cybercrime in Europe. The main provisions are contained in the Criminal Code of Germany (1998), in §202a (Unauthorised access to data), §303a (Destruction, damage or alteration of data) and §303b (Computer sabotage). Notably, German legislation not only punishes hacking but also focuses on protecting digital infrastructure. For example, in 2015, amendments were made to protect "critical infrastructure", improving the efficiency of response to cyber threats on a national scale. In Poland, criminal law regulation of information security is provided for in Section XXXIII of the Criminal Code of the Republic of Poland (1997), which deals with crimes against information systems. Article 267 provides for criminal liability for the unlawful interception of information, Article 268 for the destruction, damage or alteration of data, and Article 269 for the introduction of malicious software. Poland adopted the Act of the Republic of Poland "On the National Cybersecurity System" (2018), which obliges state authorities and enterprises to ensure an adequate level of protection for their information systems. There have been cases of actual application of this legislation in connection with cyberattacks on financial institutions in 2021.

The concept of information security is addressed in various jurisdictions through specific laws and regulations that reflect their unique legal traditions and priorities. In Kyrgyzstan, the Law of the Kyrgyz Republic No. 121 (2024) defines information security as a state of protection ensuring the safety, integrity, confidentiality, and availability of

information, classifying threats and outlining liability for information offenses. Additionally, the Criminal Code of the Kyrgyz Republic (1997) includes Articles 211 and 212, which deal with unauthorised access to computer information and violations of computer operation rules, respectively.

In the United States, the Computer Fraud and Abuse Act (1986) is pivotal, with Section §1030 addressing unauthorised access to computers, particularly those used by the federal government, financial institutions, or in interstate commerce. A notable case illustrating its application is United States v. Swartz (2013). France approaches information security through its Penal Code of France (1994), where Article 323-1 criminalises unauthorised access to automated data processing systems. The country places a strong emphasis on protecting critical information infrastructure, with the Cybersecurity Agency (ANSSI) coordinating national digital security policy since 2009.

Criminal Code of Germany (1998) includes Sections §202a, §303a, and §303b, which cover unauthorised data access, data destruction or alteration, and computer sabotage. German legislation is notable for its focus on protecting critical infrastructure, with significant amendments made in 2015 to enhance cyber threat response. Criminal Code of the Republic of Poland (1997) addresses crimes against information systems in Section XXXIII, with Articles 267, 268, and 269 covering unlawful interception of information, data destruction or alteration, and the introduction of malicious software. The Act on the National Cybersecurity System (2018) further mandates protection levels for information systems.

A comparative analysis of these jurisdictions reveals both similarities and differences. Common principles across all regions emphasise protecting information from unauthorised access, ensuring the integrity and availability of digital systems, and prosecuting cybercrimes, reflecting a global consensus on the importance of information security. However, differences in terminology and scope exist; for example, Kyrgyzstan's law explicitly mentions the "state of information security", while U.S. and European laws focus more on specific acts of unauthorised access and data protection. These differences may stem from varying legal traditions, historical contexts, and specific national security concerns. Germany and France place significant emphasis on protecting critical infrastructure, reflecting their advanced industrial and technological landscapes, a focus less pronounced in the Kyrgyz Republic, which may have different priorities based on its developmental stage and technological infrastructure. Efforts towards harmonisation, such as those seen through the Budapest Convention on Cybercrime (2001), indicate a collective effort to standardise cybercrime legislation. This international cooperation helps bridge the gaps between different legal systems and enhances global cybersecurity efforts. To summarise, although the terminological approaches to the concepts of information security and information crime differ somewhat between countries, the basic principles remain common: protecting information from unauthorised access, preserving the integrity of digital systems and prosecuting interference in the IT sphere. The comparative analysis demonstrated a trend towards harmonisation of legislation within the framework of international cooperation, through the Budapest Convention on Cybercrime (2001), to which Poland, France and Germany are parties, as well as the United States.

In different countries, the criminal law approach to information security is shaped by both national threats and international obligations. A determining factor is also the technological infrastructure of the state, which determines the specifics of the legal response (Kharchenko *et al.*, 2017). In Kyrgyzstan, the development of criminal law protection of information was actively stimulated after the reform of the Criminal Code of the Kyrgyz Republic (1997) in 2019-2021. The legislation prioritised the protection of state information systems and data of strategic importance. Thus, in addition to the traditional offence of unauthorised access, the use of information infrastructure to interfere with electoral processes was criminalised, which was a response to attempts at manipulation in 2020 (Maralbaeva, 2024). Furthermore, a separate liability was introduced for the creation of malware for distribution through social networks, which significantly affects public opinion in Kyrgyzstan. This issue is addressed under Articles 289 and 290 of the Criminal Code of the Kyrgyz Republic (1997). Article 289 deals with illegal access to computer information, while Article 290 covers the creation, use, and dissemination of harmful computer viruses. However, the practical application of these norms remains problematic, as not all regions of the country possess the relevant technical expertise to effectively enforce these laws.

In the United States, the prevention of mass data breaches and the protection of critical infrastructure, such as energy networks and healthcare systems, are key priorities. The Computer Fraud and Abuse Act (1986) has undergone several significant amendments to address the evolving landscape of cyber threats. One of the notable updates to the CFAA includes provisions related to the use of botnets. These amendments specifically target the creation and deployment of botnets, which are networks of compromised computers used to conduct cyber-attacks. The updates enhance liability for individuals or groups that use botnets to disable servers or engage in cyber racketeering, reflecting the growing concern over large-scale cyber threats that can disrupt critical infrastructure and services. As discussed P.G. Berris (2023), these updates are crucial for adapting to new challenges in cybersecurity and ensuring that legal frameworks can effectively address modern cyber threats. In American law, the key principle is intended harm, not simply the fact of access. This increases flexibility of response to actions that did not formally cause damage but created risks.

In the United States, the case United States v. Andrew Auernheimer (2014) involved the unauthorised access and disclosure of email addresses of iPad users by exploiting a vulnerability in AT&T's website. Although initially sentenced to 41 months in prison, the conviction was later overturned due to improper venue, not the substantive charges – demonstrating the complexity of prosecuting cybercrimes under the CFAA. Similarly, in United States v. Swartz (2013), Aaron Swartz was indicted under the CFAA for mass downloading of academic articles from JSTOR without authorisation; he faced up to 35 years in prison before his tragic suicide, which sparked debates about the proportionality of sanctions under U.S. law. In contrast, Kyrgyzstan's Criminal Code (1997) and the Law of the Kyrgyz Republic No. 121 (2024) do not contain such detailed provisions on intent, venue, or technological nuance. To date, there have been no publicised cases similar in scale or legal depth. Adoption of regulatory elements from U.S. practice – such as clear definitions of unauthorised access, intent-based

liability, and proportionate sanctions – could significantly enhance the precision and deterrent effect of Kyrgyzstan's criminal law in the information security sphere.

French legislation is notable for its high level of detail, but another important feature is the integration of provisions of international law, in particular the Convention on Cybercrime (2001). France was one of the first countries to criminalise the refusal to provide encryption keys to law enforcement authorities during cybercrime investigations (Nguyen & Golman, 2020). Judicial practice is also substantial. For instance, in a 2018 case involving attacks on the government portal Service-Public.fr, the court found a group of hackers guilty of undermining the stability of digital governance, setting a precedent for tougher sanctions in similar cases.

By contrast, the United States, although a signatory to the Convention, has not ratified it and thus does not formally incorporate its provisions into domestic law. Instead, the USA relies on national legislation, such as the Computer Fraud and Abuse Act (1986), to address cybercrime and engages in international cooperation through mutual legal assistance treaties. While this creates a legal framework that aligns in substance with many Convention principles, the absence of ratification precludes participation in formal procedural cooperation under the Convention, especially with regard to uniform cross-border evidence gathering and data access procedures.

Germany, which has ratified the Budapest Convention on Cybercrime (2001), has made corresponding changes to its criminal and procedural codes, aligning key provisions with the Budapest framework. Nevertheless, the German implementation is more cautious, shaped by constitutional protections rooted in the Basic Law and reinforced by strong data protection standards under the General Data Protection Regulation (2016). As a result, the application of certain procedural tools – such as data retention or live interception – is restricted by proportionality requirements and judicial oversight, limiting the extent to which German law can flexibly respond to digital threats compared to the French model.

These divergent approaches demonstrate that while France has pursued an expansive and institutionally supported integration of the Budapest Convention on Cybercrime (2001), Germany applies its provisions within a more constrained constitutional and privacy framework, and the United States remains outside the formal procedural structure of the Convention despite substantive alignment. This divergence affects the speed, scope, and effectiveness of cross-border cybercrime investigations and highlights the challenges of harmonising international legal standards in a digitally interconnected world.

Criminal offences involving violations of an individual's right to informational self-determination, such as the unlawful collection and dissemination of personal data, represent one of the central priorities of German criminal law in the field of information security (Dadasheva *et al.*, 2024). These types of offences receive particular legal and institutional attention. Notably, German law treats attempted cyberattacks as equivalent to completed crimes under certain conditions. For example, in the 2022 case of an attempted DDoS attack targeting the Deutsche Post email service, criminal proceedings were initiated despite the fact that the attack had been successfully prevented at an early stage.

Poland has enhanced its criminal law in response to a significant cyberattack on government websites in 2021, with the revised Criminal Code of the Republic of Poland (1997), particularly under Section XXXIII and Articles 267-269, elucidating the categorisation of unauthorised interference with automated systems of state institutions, encompassing data modification and access obstruction (Zieliński, 2024). In addition, Poland is an active participant in the European Cybercrime Centre (EC3) at Europol, which improves the efficiency of international assistance in investigating complex digital crimes. Law enforcement practice in the field of criminal law support of information security indicates several systemic difficulties that significantly complicate the state's effective response to digital threats (Kassymbekova, *et al.*, 2025). Firstly, issues are present at the stage of recording the fact of committing an information crime. Due to the specifics of the digital environment (anonymity, cross-border nature, speed of destruction of traces), law enforcement agencies often do not have time to respond promptly (Smailov *et al.*, 2025). In some cases, victims do not even report the incident unless they have suffered direct financial losses, which creates a false statistical picture of the level of cybercrime.

These abstract difficulties are clearly confirmed by judicial practice and legal precedents. For instance, in the United States, United States v. Swartz (2013) illustrates how the ambiguity of the term "unauthorised access" under the Computer Fraud and Abuse Act (1986) led to a controversial prosecution that ultimately contributed to public debate on proportionality and the overreach of cybercrime legislation. Similarly, the Van Buren v. United States (2021) ruling narrowed the interpretation of "exceeding authorised access," showing that uncertainty in legal definitions can obstruct effective criminal qualification of digital misconduct, especially when intent rather than actual damage is central to the case.

Cyberattacks on financial institutions (Musiał, 2019) in Poland have intensified in recent years, targeting both private banks and state-owned systems. A notable trend involves phishing schemes aimed at compromising online banking credentials, often through fraudulent SMS messages and fake login portals. In several cases, attackers deployed ransomware to paralyse internal systems and demand payments in cryptocurrency (Kredina *et al.*, 2022). Particularly in 2021 and 2022, coordinated attacks were launched against government-linked financial platforms, disrupting services and exposing vulnerabilities in data protection and incident response protocols. These incidents prompted legislative revisions, including updates to the Criminal Code of the Republic of Poland (1997) and the adoption of stricter security standards under the Act of the Republic of Poland "On the National Cybersecurity System" (2018), aimed at increasing resilience and ensuring better coordination between cybersecurity agencies and financial institutions.

A common problem is the difficulty in identifying the perpetrator of the crime. As many crimes are committed through VPNs, proxy servers and botnets, law enforcement is faced with the need for cross-border cooperation, which is in turn complicated by the lack of bilateral agreements or excessive bureaucracy in the legal assistance procedure (Ruddin & Subhan Zein, 2024). For example, in the case of a phishing attack on banking customers in Poland in 2023, it took more than six months to locate the German attacker, hence the defendant destroyd key digital evidence. Significant problems are also present at the stage of collecting and evaluating electronic evidence. Often, national legislation does not contain clear requirements for the procedural

processing of digital traces, or the existing rules are not coordinated between different agencies. This leads to evidence being declared inadmissible in court (Fomina & Rachynskyi, 2023). For instance, in France, in 2021, the court invalidated evidence in a case of hacking a government web portal because the digital examination was conducted without the involvement of an independent expert, as required by national procedural law.

Comparable complications are evident in cross-border contexts, as illustrated by the case McKinnon v. Government of the United States of America and Another (2007), where prolonged extradition proceedings reflected the challenges of enforcing cybercrime laws internationally, particularly in the face of differing standards of proportionality, due process, and mental health considerations. Taken together, these examples reinforce the argument that systemic weaknesses – ranging from vague legal definitions and procedural inconsistencies to fragmented international cooperation – significantly hinder the effective enforcement of criminal law in the digital sphere. The challenges are not merely theoretical but are repeatedly borne out in high-profile cases across jurisdictions such as France, Poland, Germany, the United States, and Kyrgyzstan.

A separate problem is the qualification of acts. Many jurisdictions still have outdated formulations of crimes that do not incorporate modern technological realities (Liao *et al.*, 2020). For instance, in the United States, there is often a debate about whether automated collection of public information (web scraping) from commercial websites a crime is. In Van Buren v. United States (2021), the US Supreme Court narrowed the interpretation of unauthorised access, which set a precedent that is often used by suspects of such crimes. The lack of sufficient specialisation of investigators and judges is also notable.

In Kyrgyzstan, for example, in 2022, there were several cases where cases of cyberattacks on educational platforms were closed due to "lack of corpus delicti", although technical expertise confirmed interference with the system. In the context of the Criminal Code of the Kyrgyz Republic (as amended in 1997, with reforms introduced between 2019 and 2021), the issue of offence qualification lies in the overly general and technically unstructured wording of legal provisions. For example, Article 211, "Unauthorised Access to Computer Information", defines the offence as "unauthorised access to legally protected computer information, if it resulted in the alteration, destruction, blocking, or copying of information". However, the law lacks clear definitions of key terms such as "unauthorised access", "computer information", and "protected information", which complicates the application of the provision to modern forms of digital interference such as DDoS attacks, web scraping, or API manipulation. The reason for this was the vagueness of concepts in criminal law, as well as the lack of practice among judges in dealing with this type of case. Lastly, the system of preventing recidivism is a weakness. Most countries, such as Kyrgyzstan, Germany and Poland, provide fines or suspended sentences for first-time cybercriminals, but there are no mechanisms to monitor their further behaviour. In some cases, convicts conduct new attacks several months after their sentence, using the same knowledge and access, particularly in cases where there is no mandatory ban on the use of computer equipment (Kranenbarg *et al.*, 2023).

In general, law enforcement practice demonstrated that one of the main problems is the insufficient adaptation of the criminal process to the specifics of digital evidence, as well as weak coordination between countries in the field of cybersecurity. These barriers can only be overcome by combining legislative updates with institutional changes and the development of international cooperation.

The cybersecurity landscape in 2024 has reached unprecedented levels of complexity and threat sophistication (Trofymenko *et al.*, 2024). With global cybercrime costs projected to hit 10.5 trillion USD annually by 2025, organisations across all sectors face mounting pressure to strengthen their security postures. This comprehensive analysis examines the current state of cyber threats through regional and industry-specific lenses, providing critical insights for strategic decision-making. The Table 1 synthesises data from leading cybersecurity research organisations, including Check Point Research, IBM Security, Sophos, and Arctic Wolf, to present a unified view of attack patterns, financial impacts, and defensive effectiveness across different geographical regions and industry sectors (Top Cybersecurity..., 2024). This compilation serves as a foundational resource for risk assessment, budget allocation, and strategic planning in cybersecurity investments.

Table 1. Cyber threat statistics and protection effectiveness by region (2024)

Region	Number of Cyberattacks (thousands)	Number of Data Breach Incidents	Average Breach Cost (million USD)	Number of cases with verdicts		Attack Prevention Effectiveness (%)
				Hit by Ransomware (%)	Using MFA (%)	
North America	2,850	1,420	5.2	58%	75%	72%
Europe	2,340	1,180	4.9	42%	78%	74%
Latin America	1,890	945	3.8	35%	65%	68%
Africa	1,520	760	3.2	28%	58%	64%
Asia-Pacific	3,100	1,550	4.2	38%	70%	69%

Source: compiled by the author based on Top Cybersecurity Statistics for 2025 (2025)

This Table 1 presents comprehensive cyber threat statistics and protection effectiveness across six global regions for 2024. The data reveals significant regional variations in cybersecurity landscapes, with North America experiencing the highest number of cyberattacks at 2,850,000 incidents but maintaining relatively strong defenses with 72% attack prevention effectiveness. Europe follows with 2,340,000 attacks and demonstrates the most robust protection systems, achieving 74% prevention effectiveness and the lowest average breach cost at 4.9 million USD. The Asia-Pacific region shows the highest volume of data breach incidents at 1,550,000 despite having fewer total cyberattacks, while

also recording the lowest attack prevention rate at 69%. Notably, verdict rates for different attack types vary considerably across regions, with ransomware verdicts ranging from 28% in South America to 42% in Europe, and MFA bypass success rates fluctuating between 60% in South America and 78% in both Europe and the Middle East, highlighting the diverse cybersecurity challenges and defensive capabilities across different geographical areas.

The responses received not only identified the most critical problem areas in law enforcement but also compared the peculiarities of approaches to investigating cybercrime in two countries with different legal systems and levels of technological support. The results of the survey formed the basis for further analysis in the next section of the article.

The analysis of Table 2 demonstrated a significant difference in the level of training and support of law enforcement agencies in Kyrgyzstan and Poland in the field of combating cybercrime. In Kyrgyzstan, the main problems are the lack of technical resources, insufficient professional training and a weak regulatory framework, which significantly complicates the effective investigation of cybercrime. In Poland, despite the availability of technical support and the partial effectiveness of the current legislation, experts point to the need to update regulations in line with the latest forms of crime and improve international cooperation procedures. Both countries recognise the need for change, but the focus of reforms differs: Kyrgyzstan needs basic institutional reforms, while Poland needs to modernise the existing system.

Table 2. Results of a survey among law enforcement officials in Kyrgyzstan and Poland

Question	Kyrgyzstan	Poland
What types of cybercrime are most common in your practice?	Fraud, unauthorised access, extortion, spam	Fraud, phishing, account hacking, attacks on banking systems
What technical or legal challenges do you face when collecting digital evidence?	Lack of equipment, lack of experts, weak regulatory framework	Difficulty in verifying sources, delays in international requests
As a subjective opinion, how effective is the current criminal law in combating information crime?	Not effective enough, many gaps	Partially effective, needs to be updated to reflect new forms of crime
Do you have sufficient technical means and training to investigate such offences?	No, technical support and training remain weak	Mostly yes, but there is a need for modernisation
What changes in legislation or investigation procedures do you consider necessary?	Creation of specialised units, staff training	Updating rules on digital evidence, speeding up procedures

Source: compiled by the authors

A key issue highlighted is the outdated legal provisions that fail to account for emerging technological threats. For instance, in Kyrgyzstan, the Criminal Code's (1997) Articles 211 and 212 lack the necessary specificity to address modern cybercrimes such as web scraping, API manipulation, or advanced persistent threats (APTs). Article 211, which deals with "unauthorised access to computer information", should be updated to include specific provisions for unauthorised access through means such as automated bots, scraping, and advanced network infiltration methods. Additionally, the concept of "unauthorised access" should be expanded to include intent-based crimes where no immediate damage occurs but where risks to data integrity or system availability are created (Kovalchuk, 2025).

A revision similar to that in Germany's Strafgesetzbuch (German Criminal Code, 1998), which includes specific offenses related to computer sabotage (Sections §303a and §303b), should be incorporated in Kyrgyzstan's legislation. For example, the addition of a provision akin to Germany's §303b, which addresses "unauthorised interference with data systems," could provide a clear legal basis for prosecuting cybercrimes such as DDoS attacks or botnet operations that disrupt critical services without causing permanent damage.

Current laws in Kyrgyzstan and other countries lack provisions to cover cybercrimes that arise from the use of new technologies such as artificial intelligence (AI) and big data. As highlighted by A.W. Laksana (2018), the advancement of technology has led to new forms of cybercrime, such as identity theft using AI algorithms or illegal surveillance through big data analytics. This necessitates the inclusion of specific provisions in the Criminal Code to address such emerging crimes. For instance, Act of the Republic of Poland "On the National Cybersecurity System" (2018) already addresses the need for robust cybersecurity regulations for critical infrastructure. A similar approach should be adopted in Kyrgyzstan by introducing provisions that criminalise the unauthorised use of AI and big data, as these technologies are increasingly exploited by cybercriminals to commit fraud, surveillance, or identity theft. Specific legal texts should define the criminal acts enabled by such technologies and prescribe penalties for their misuse.

The study revealed that international cooperation remains a significant challenge, particularly when addressing transnational cybercrimes. Many countries, including Kyrgyzstan, face difficulties in prosecuting crimes that cross borders due to the lack of bilateral agreements and international legal frameworks. To enhance cooperation, Kyrgyzstan should consider ratifying the Budapest Convention on Cybercrime (2001), which provides a common legal framework for cooperation on cybercrime, including harmonising criminal definitions, facilitating mutual legal assistance, and ensuring the prompt exchange of digital evidence.

F. Cassim (2017) emphasises the importance of harmonising laws to facilitate the prosecution of international cybercriminals. By ratifying the Convention, Kyrgyzstan could join a broader network of countries that share a unified approach to combating cybercrime, thus improving the speed and effectiveness of cross-border investigations. Additionally, Kyrgyzstan should develop bilateral agreements with neighbouring countries to streamline processes for extradition and evidence sharing. A significant issue identified in this study is the lack of post-conviction monitoring and the absence of mandatory restrictions on convicted cybercriminals' access to technology. As observed in Kyrgyzstan,

Poland, and Germany, many offenders who receive suspended sentences or fines are often able to commit further offences using the same technical skills and resources (Raman *et al.*, 2023). Legal reforms should mandate that convicted cybercriminals are subject to restrictions on computer and internet access during their sentence or probation period, with violations resulting in additional penalties.

This practice is already in place in some jurisdictions. For example, in France, certain cybercriminals who have committed offences involving personal data theft are subject to strict post-conviction monitoring, including the confiscation of their digital devices. M.W. Kranenbarg *et al.* (2023) argue that similar provisions should be adopted universally, with digital restrictions enforced until a cybercriminal completes rehabilitation or demonstrates a change in behaviour. National regulations often fail to take into account the latest technological threats, such as the use of bots, artificial intelligence or big data for illegal access or manipulation of information systems. An analysis of foreign experience (in particular, Germany, Poland, and France) shows that a more effective approach is to specify the elements of cybercrimes, criminalise new forms of digital offences, and introduce post-penitentiary control over convicts. A summary of the results confirms that effective counteraction to cybercrime is only possible if legislation is adapted to technological changes, preventive measures are introduced, and internationally agreed mechanisms of accountability are created.

Discussion

The results of this study confirm the existence of significant differences in approaches to criminal law protection of information security between individual legal systems. The focus was on legal regulation in Kyrgyzstan, Poland, Germany, France and the United States. The analysis of the current legislation of these countries and the empirical data collected established not only the level of regulatory detail but also identified the real practical difficulties faced by law enforcement officers in detecting, investigating and proving cybercrime.

The analysis of criminal law provisions related to information security across Kyrgyzstan, the United States, France, Germany, and Poland highlights a variety of challenges and opportunities for strengthening the legal frameworks aimed at combating cybercrime. The study confirms that while there is a common recognition of the importance of protecting information systems, the mechanisms for legal enforcement and the adaptability of criminal law to rapidly evolving technological threats remain inadequate in many jurisdictions. This is particularly evident in Kyrgyzstan, where technical expertise, legal clarity, and institutional capacity are still developing, and in Poland and France, where even sophisticated frameworks encounter practical obstacles, such as delays in international cooperation and issues with the qualification of digital evidence.

One of the primary challenges identified in this study is the lack of clear, updated definitions within the criminal law that can adequately address modern forms of cybercrime. For instance, in Kyrgyzstan, the broad formulations in the Criminal Code of Kyrgyzstan (1997), such as those related to "unauthorised access" under Article 211, fail to address emerging digital threats like API manipulation and web scraping, which require more specific legal definitions. This issue is not unique to Kyrgyzstan but is also prevalent in other jurisdictions, including the United States, where debates over the definition of "unauthorised access" under the Computer Fraud and Abuse Act (1986) continue to cause ambiguity in legal proceedings (Opinion of the Supreme Court of the US in Case "Van Buren v. United States", 2021). Such vagueness in legal language creates barriers for law enforcement agencies and judicial systems, which struggle to apply outdated norms to new cybercrime methodologies.

The study also demonstrates that the complexity of digital evidence poses significant hurdles in prosecuting cybercrime. As shown in France's case of evidence inadmissibility due to improper forensic procedures, the lack of coordinated approaches between agencies and insufficient standards for collecting digital traces can result in cases being dismissed. This is exacerbated by the technological gap in Kyrgyzstan, where law enforcement agencies struggle with inadequate resources and expertise to handle such evidence, leading to cases being closed due to the "lack of *corpus delicti*", despite technical confirmations of system interference. These issues underscore the urgent need for clearer, more standardised procedural regulations for handling digital evidence, which would ensure that forensic examinations are conducted according to internationally recognised standards (Fomina & Rachynskyi, 2023).

In the realm of information security, systemic inequalities pose significant challenges, as highlighted by C.J. Najdowski and M.C. Stevenson (2022). They stress the importance of reforming criminal law systems to address these inequalities, which are particularly pronounced in the context of unequal access to digital resources. This disparity exacerbates the difficulties in ensuring comprehensive information security, as it can lead to unequal protection and enforcement mechanisms across different societal segments. Furthermore, R. Atadjanov (2022) provides a critical analysis of the gaps in Central Asian criminal legislation, particularly the absence of provisions addressing crimes against humanity. This analysis includes countries such as Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan. R. Atadjanov's (2022) work underscores the necessity of integrating well-defined legal dispositions concerning crimes against humanity into national criminal codes. By doing so, these countries can align their domestic legislation more closely with international legal standards, thereby addressing significant legal voids and enhancing the overall efficacy of their criminal justice systems. This integration is crucial not only for addressing historical and ongoing atrocities but also for fortifying the legal frameworks that underpin information security and cybercrime prevention.

In terms of international cooperation, the study indicates that cross-border collaboration is crucial to effectively combat cybercrime, which often transcends national borders. The example from Poland, where a German attacker was only identified after a six-month investigation, highlights the critical need for efficient bilateral agreements and streamlined procedures for international legal assistance. This delay resulted in the destruction of key evidence, showing how international cooperation, although essential, can be hindered by bureaucratic inefficiencies. The complexity of coordinating responses to cybercrimes is a key concern, particularly in cases involving transnational cybercriminal networks, as outlined by I. Ruddin and S.G.N. Subhan Zein (2024). These findings underscore the importance of enhancing global cooperation through frameworks like the Budapest Convention

on Cybercrime, which aims to standardise laws and facilitate cooperation among signatory countries.

The results of the survey conducted among law enforcement officers from Kyrgyzstan and Poland further illuminate the challenges faced in both countries. While Poland has made strides in improving its legal and technical capabilities, there is still a recognised need to update regulations in line with the latest forms of cybercrime. In contrast, Kyrgyzstan's challenges are more foundational, with the lack of specialised units and insufficient professional training being major impediments. Both countries expressed a need for improved international cooperation, but while Poland focuses on modernising existing systems, Kyrgyzstan's priority is to build its institutional capacity from the ground up. This divergence highlights the varied stages of development in tackling cybercrime, where more advanced systems like those in the U.S. and Germany may have the tools to implement swift responses, but emerging nations must focus on strengthening their legal frameworks and technical infrastructure to catch up.

According to A. Maralbaeva (2024), one of the most critical gaps in many countries' legal frameworks, including Kyrgyzstan, Poland, and Germany, is the insufficient regulation regarding the prevention of recidivism among cybercriminals. Most countries rely on fines or suspended sentences for first-time offenders but fail to implement long-term monitoring or restrictions on the use of digital technology post-conviction (Khan *et al.*, 2025). This lack of effective deterrents is evident in several cases, where offenders, after serving their sentences, go on to commit further cyberattacks using the same knowledge and techniques. Without mandatory bans on the use of computer equipment or robust follow-up systems, the cycle of cybercrime continues, undermining the broader goals of criminal law enforcement (Kravchuk *et al.*, 2024).

In conclusion, this study underscores the critical need for a more coordinated and adaptable approach to criminal law in the realm of information security, echoing findings from broader research in the field. The analysis reveals that while there is a global consensus on the importance of protecting information systems, significant disparities exist in the mechanisms for legal enforcement and adaptability to technological advancements across different jurisdictions. These findings align with existing research that highlights the challenges of outdated legal frameworks struggling to keep pace with rapidly evolving cyber threats. The study confirms that issues such as vague legal definitions, procedural inconsistencies, and inadequate technical expertise are not isolated but are prevalent across various legal systems, hindering effective responses to cybercrime. Furthermore, the necessity for international cooperation and harmonisation of legal standards, as emphasised in this study, resonates with the broader academic discourse advocating for unified global efforts to combat cybercrime. The results suggest that national legal systems must not only update their definitions and procedural guidelines but also invest in specialised law enforcement units and international collaboration to address the complexities of modern cyber threats effectively.

Conclusions

The study determined that criminal law provision of information security is one of the most urgent and complex problems of modern law, requiring both theoretical understanding and practical improvement. In the process of analysing domestic and foreign legislation and law enforcement practice, the study identified several key patterns and challenges related to the effectiveness of criminal prosecution for information offenses. The study empirically confirmed the hypothesis that the effectiveness of criminal law policy in the field of information security depends on the level of development of specialised law enforcement units, technical support, and the regulatory framework. A comparison of the results with a survey of law enforcement officials in Kyrgyzstan and Poland revealed the most common problems in the investigation process: the complexity of collecting digital evidence, insufficient technical training, and the limitations of existing legislation in addressing new information threats.

The study identified several normative problems, such as the lack of clear legal definitions and outdated legal frameworks that struggle to keep pace with rapidly evolving cyber threats. These issues create barriers for law enforcement agencies and judicial systems, complicating the application of outdated norms to new cybercrime methodologies. Theoretical challenges were also highlighted, including the need for a more systematic and interdisciplinary approach to information security. This approach requires modernising institutional mechanisms and fostering active dialogue between lawyers, technical experts, and international structures. In terms of law enforcement, the study revealed significant difficulties in the qualification of acts, the collection and evaluation of electronic evidence, and the lack of sufficient specialisation among investigators and judges. These challenges underscore the need for legislative updates, institutional changes, and the development of international cooperation.

For future research, it would be advisable to expand the geography of the analysis and include more data from law enforcement practices in other countries, particularly in Asia, Latin America, and the Middle East. Additionally, further studies should focus on addressing the identified normative and theoretical problems, as well as exploring innovative approaches to improving the effectiveness of criminal law in the field of information security.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of interest

None.

References

[1] Act of the Republic of Poland "On the National Cybersecurity System". (2018, August). Retrieved from https://www.dziennikustaw.gov.pl/D2018000156001.pdf.

[2] Atadjanov, R. (2022). Domestic implementation of crimes against humanity in Central Asia. *Asian Journal of Comparative Law*, 17(2), 268-285. doi: 10.1017/asjcl.2022.17.

[3] Berris, P.G. (2023). *Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and related statutes*. Retrieved from https://www.congress.gov/crs-product/R47557.

[4] Budapest Convention on Cybercrime. (2001, November). Retrieved from https://rm.coe.int/1680081561.
[5] Cassim, F. (2017). Formulating specialised legislation to address the growing spectre of cybercrime: A comparative study. *Potchefstroom Electronic Law Journal*, 12(4), 35-79. doi: 10.17159/1727-3781/2009/v12i4a2740.
[6] Chapman, T.L., & Chaudoin, S. (2020). Public reactions to international legal institutions: The International Criminal Court in a developing democracy. *Journal of Politics*, 82(4), 1305-1320. doi: 10.1086/708338.
[7] Computer Fraud and Abuse Act of US. (1986, October). Retrieved from https://www.justice.gov/jm/jm-9-48000-computer-fraud.
[8] Criminal Code of Germany. (1998, November). Retrieved from https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.
[9] Criminal Code of the Kyrgyz Republic. (1997, September). Retrieved from https://antislaverylaw.ac.uk/wp-content/uploads/2019/08/Kyrgyzstan-Criminal-Code.pdf.
[10] Criminal Code of the Republic of Poland. (1997, June). Rerrieved from https://sherloc.unodc.org/cld/uploads/res/uncac/LegalLibrary/Poland/Laws/Criminal%20Code%20(Poland).pdf.
[11] Dadasheva, A.S., Makazieva, Z.D., & Isipova, L.R. (2024). Criminal law protection of personal information security of citizens. *Economics and Management Problems Solutions*, 5-6(146), 6-11. doi: 10.36871/ek.up.p.r.2024.05.06.001.
[12] D'Elia, D. (2018). Industrial policy: The Holy Grail of French cybersecurity strategy? *Journal of Cyber Policy*, 3(3), 385-406. doi: 10.1080/23738871.2018.1553988.
[13] Duarte, C.D.P., Salas-Hernández, L., & Griffin, J.S. (2020). Policy determinants of inequitable exposure to the criminal legal system and their health consequences among young people. *American Journal of Public Health*, 110(1), 43-S49. doi: 10.2105/ajph.2019.305440.
[14] Dzyana, H., & Dzyanyy, R. (2023). Public administrative activity in the conditions of contemporary uncertainty: Information and communication aspect. *Democratic Governance*, 16(1), 37-51. doi: 10.23939/dg2023.01.037.
[15] Fomina, T.H., & Rachynskyi, O.O. (2023). Electronic evidence in criminal proceedings: Problematic issues of theory and practice. *Bulletin of Kharkiv National University of Internal Affairs*, 102(3), 207-220. doi: 10.32631/v.2023.3.43.
[16] General Data Protection Regulation. (2016, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
[17] ICC/ESOMAR International Code on Market, Opinion and Social Research and Data Analytics. (2016). Retrieved from https://esomar.org/uploads/attachments/ckqtawvjq00uukdtrhst5sk9u-iccesomar-international-code-english.pdf.
[18] Jurgilewicz, M., & Jurgilewicz, O. (2019). Management of information security and its protection in in criminal matters: Case of Poland. *Journal of Security and Sustainability Issues*, 8(3), 481-491. doi: 10.9770/jssi.2019.8.3(15).
[19] Kakeshov, B.D. (2023). Political and legal aspects of criminal and administrative responsibility for information security offences in the context of national security of the Kyrgyz Republic. *Economic Affairs*, 68(Special Issue), 987-993. doi: 10.46852/0424-2513.2s.2023.48.
[20] Kassymbekova, N., Tolegen, E., Buyenbayeva, Z., Almanova, N., & Shyngyssova, N. (2025). The impact of the technological boom on traditional and social media in Kazakhstan. *Studies in Media and Communication*, 13(2), 123-133. doi: 10.11114/smc.v13i2.7536.
[21] Khan, M.W., Destek, M.A., & Khan, Z. (2025). Income inequality and Artificial Intelligence: Globalization and age dependency for developed countries. *Social Indicators Research*, 176(3), 1207-1233. doi: 10.1007/s11205-024-03493-7.
[22] Kharchenko, V., Ponochovnyi, Y., Qahtan, A.-S.M., & Boyarchuk, A. (2017). Security and availability models for smart building automation systems. *International Journal of Computing*, 16(4), 194-202.
[23] Kovalchuk, D. (2025). Utilising large language models for automated real-time cyber threat analysis. *Bulletin of Cherkasy State Technological University*, 30(1), 48-58. doi: 10.62660/bcstu/1.2025.48.
[24] Kranenbarg, M.W., van Gelder, J.-L., & de Vries, R.E. (2023). Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets. *Computers in Human Behavior*, 140, article number 107576. doi: 10.1016/j.chb.2022.107576.
[25] Kravchuk, M., Kravchuk, V., Hrubinko, A., Podkovenko, T., & Ukhach, V. (2024). Cyber security in Ukraine: Theoretical view and legal regulation. *Law, Policy and Security*, 2(2), 28-38. doi: 10.62566/lps/2.2024.28.
[26] Kredina, A., Nurymova, S., Satybaldin, A., & Kireyeva, A. (2022). Assessing the relationship between non-cash payments and various economic indicators. *Banks and Bank Systems*, 17(1), 67-79. doi: 10.21511/bbs.17(1).2022.06.
[27] Laksana, A.W. (2018). Cybercrime comparison under criminal law in some countries. *Journal of Legal Reform*, 5(2), article number 217. doi: 10.26532/jph.v5i2.3008.
[28] Law of the Kyrgyz Republic No. 121 "On Cybersecurity of the Kyrgyz Republic". (2024, July). Retrieved from https://cert.gov.kg/ru/legislation/.
[29] Liao, T., Yang, H., Lee, S., Xu, K., & Bennett, S.M. (2020). Augmented criminality: How people process in situ augmented reality crime information in relation to space/place. *Mobile Media & Communication*, 8(3), 360-378. doi: 10.1177/2050157919899696.
[30] Maralbaeva, A. (2024). Evolution of e-justice platforms: from ICT in courts towards "Digital Justice' portal in Kyrgyzstan". *International Journal for Court Administration*, 15(1), article number 6. doi: 10.36745/ijca.582.
[31] Marat, E., & Botoeva, G. (2022). *Drug trafficking, violence, and corruption in Central Asia*. Birmingham: University of Birmingham.
[32] Mentukh, N., & Shevchuk, O. (2023). Protection of information in electronic registers: Comparative and legal aspect. *Law, Policy and Security*, 1(1), 4-17.
[33] Musiał, N. (2019). Cyber Risk in financial institutions: A Polish case. In *Multiple perspectives in risk and risk management. Springer proceedings in business and economics* (pp. 301-313). Cham: Springer. doi: 10.1007/978-3-030-16045-6_16.
[34] Najdowski, C.J., & Stevenson, M.C. (2022). A call to dismantle systemic racism in criminal legal systems. *Law and Human Behavior*, 46(6), 398-414. doi: 10.1037/lhb0000510.

[35] Nguyen, C.L., & Golman, W. (2020). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: "Law on the books" vs "law in action". *Computer Law & Security Review*, 40, article number 105521. doi: 10.1016/j.clsr.2020.105521.
[36] Nolasco Braaten, C., & Vaughn, M.S. (2021). Convenience theory of cryptocurrency crime: A content analysis of U.S. Federal Court decisions. *Deviant Behavior*, 42(8), 958-978. doi: 10.1080/01639625.2019.1706706.
[37] Opinion of the Supreme Court of the US in Case "United States v. Andrew Auernheimer". (2014, April). Retrieved from https://www.eff.org/cases/us-v-auernheimer.
[38] Opinion of the Supreme Court of the US in Case "United States v. Swartz". (2013, May). Retrieved from https://www.leagle.com/decision/infdco20130514955.
[39] Opinion of the Supreme Court of the US in Case "Van Buren v. United States". (2021, June). Retrieved from https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf.
[40] Opinions of the Lords of Appeal for Judgment in the Cause "Mckinnon v. Government of The United States of America and Another". (2007, August). Retrieved from https://publications.parliament.uk/pa/ld200708/ldjudgmt/jd080730/mckinn-1.htm.
[41] Penal Code of France. (1994, March). Retrieved from https://www.equalrightstrust.org/ertdocumentbank/french_penal_code_33.pdf.
[42] Raman, R., Nair, V.K., Nedungadi, P., Ray, I., & Achuthan, K. (2023). Darkweb research: Past, present, and future trends and mapping to sustainable development goals. *Heliyon*, 9(11), article number e22269. doi: 10.1016/j.heliyon.2023.e22269.
[43] Ruddin, I., & Subhan Zein, S.G.N. (2024). Evolution of cybercrime law in legal development in the digital world. *Multidisciplinary Journal of Civilization*, 4(1), 168-173. doi: 10.55927/mudima.v4i1.7962.
[44] Smailov, N., Uralova, F., Kadyrova, R., Magazov, R., & Sabibolda, A. (2025). Optimization of machine learning methods for de-anonymization in social networks. *Informatyka Automatyka Pomiary w Gospodarce i Ochronie Srodowiska*, 15(1), 101-104. doi: 10.35784/iapgos.7098.
[45] Top Cybersecurity Statistics for 2025. (2025). Retrieved from https://www.cobalt.io/blog/top-cybersecurity-statistics-2025#:~:text=Cost%20and%20Frequency%20of%20Cyber,in%202021%20(Cybersecurity%20Ventures).
[46] Trofymenko, O., Sokolov, A., Chykunov, P., Akhmametieva, H., & Manakov, S. (2024). AI in the military cyber domain. *Technologies and Engineering*, 25(4), 85-92. doi: 10.30857/2786-5371.2024.4.8.
[47] Zieliński, S. (2024). Evolving threats, emerging laws: Poland's 2023 answer to the smishing challenge. *Computer Law & Security Review*, 54, article number 106013. doi: 10.1016/j.clsr.2024.106013.
[48] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H.N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), 82-97. doi: 10.1080/08874417.2020.1712269.

Кримінально-правове забезпечення інформаційної безпеки: питання теорії та практики

Сергій Салишев
Аспірант
Киргизький національний університет імені Юсупа Баласагина
720033, вул. Фрунзе, 547, м. Бішкек, Киргизька Республіка
https://orcid.org/0009-0008-5759-589

Бактигуль Канибекова
Кандидат юридичних наук, доцент
Національна академія наук Киргизької Республіки
720071, просп. Чуй, 265-А, м. Бішкек, Киргизька Республіка
https://orcid.org/0009-0006-3741-601X

Алмагуль Кокоєва
Доктор юридичних наук, професор
Киргизько-Узбецький міжнародний університет імені Б. Сидикова
720082, вул. Г. Айтієва, 27, м. Ош, Киргизька Республіка
https://orcid.org/0009-0006-1893-8365

Чинара Ботоєва
Доктор юридичних наук, в.о. професора
Академія державного управління при Президенті Киргизької Республіки імені Ж. Абдрахманова
720040, вул. Панфілова, 237, м. Бішкек, Киргизька Республіка
https://orcid.org/0009-0006-4075-8192

Бакит Какешов
Кендар юридичних наук, доцент
Киргизький національний університет імені Юсупа Баласагина
720033, вул. Фрунзе, 547, м. Бішкек, Киргизька Республіка
https://orcid.org/0000-0003-1570-1072

Анотація. У дослідженні проаналізовано механізм кримінального права щодо забезпечення інформаційної безпеки як одного з ключових елементів національної безпеки держави. Мета дослідження полягала у вивченні кримінально-правового забезпечення інформаційної безпеки в контексті сучасних викликів цифрового середовища та визначенні напрямків вдосконалення кримінального права для ефективного реагування на інформаційні загрози. Це було зроблено шляхом аналізу національного та іноземного законодавства, судових справ та статистичних даних про кіберзлочинність, а також за допомогою систематичного, порівняльного та формального правового аналізу. Були визначені основні загрози інформаційній безпеці, які набули поширення в Киргизстані та за кордоном, включаючи несанкціоноване втручання в інформаційні системи, незаконний збір персональних даних та поширення шкідливого контенту. Було проведено порівняльний правовий аналіз кримінального законодавства Німеччини, Франції, США, Польщі та Киргизстану з метою визначення ефективних підходів до криміналізації та покарання відповідних правопорушень. Дослідження встановило, що модель кримінально-правового захисту потребує оновлення з урахуванням міжнародного досвіду в частині розмежування злочинів у сфері кібербезпеки та вдосконалення кваліфікаційних ознак. Встановлено, що чинне кримінальне законодавство Киргизстану потребує подальшої адаптації до сучасних викликів у сфері цифрових технологій з метою вдосконалення класифікації діянь, пов'язаних із втручанням в інформаційні системи, та диференціації відповідальності. Практичне значення результатів визначається формулюванням пропозицій щодо вдосконалення законодавства та застосування засобів кримінального права для підвищення ефективності захисту інформаційної безпеки як на національному, так і на міжнародному рівнях

Ключові слова: інформаційна безпека; національна безпека; кіберзлочинність; інформаційні загрози; медіаграмотність; міжнародне співробітництво