RESEARCH ON THE CHARACTERISTICS OF CRIMINAL OFFENSES IN THE FIELD OF INFORMATION AND COMMUNICATIONS

Yuldashev R., Kalpeyeva Z.,

Satpayev University, Almaty, Kazakhstan

e-mail: 010525501027-M@stud.satbayev.university,

z.kalpeyeva@satbayev.university

Abstract. The rapid development of digital technologies and the expansion of internet access in Kazakhstan have led to a surge in cybercrimes, which pose significant risks to society and individuals. This research investigates the characteristics of criminal offenses in the area of information and communications, highlighting trends, legislation, and the role of cybersecurity measures in mitigating these risks. By analyzing data from various sources and evaluating criminal statistics, the paper explores the need for enhanced laws and technological frameworks to address these crimes.

Keywords. Cybercrime, Information Security, Legislation, Criminal Offenses, Cybersecurity

Introduction. The digital transformation of Kazakhstan has resulted in a greater integration of technology in everyday life, making it vulnerable to various forms of cybercrimes. The increase in internet penetration, which now exceeds 89% of the population in Kazakhstan, has amplified the risks of cybercrimes such as unauthorized access to information systems, data theft, and the spread of malicious software. The criminal law framework in Kazakhstan, including the Criminal Code, provides the necessary legal grounds for prosecuting cybercriminals. However, there is still a growing need to enhance these regulations in response to new and emerging digital threats.

Methodology. This research employs both qualitative and quantitative methods. Statistical data on the prevalence of cybercrimes in Kazakhstan was analyzed, and an assessment of the existing legal framework was conducted. Additionally, the role of cybersecurity measures implemented by the government and private sector was evaluated. Various reports and publications were reviewed to understand the current landscape of cybercrimes and evaluate the effectiveness of legal and technological countermeasures.

Results. According to a report from the digital portal in 2022, more than 89% of Kazakhstan's population actively uses the internet, reflecting a high degree of digital engagement. This statistic underscores the growing reliance on digital technologies, which increases the vulnerability to cybercrimes. These findings indicate that a significant portion of the population participates in the digital space, highlighting the urgency of addressing cybersecurity risks [1]. The structure of criminal offenses in Kazakhstan's information and communications sector reveals a substantial focus on crimes such as unauthorized access to information or information systems (Article 205 of the Criminal Code of Kazakhstan), the illegal destruction or modification of information (Article 206), and the creation and distribution of malicious programs (Article 233) [2]. These crimes have contributed significantly to the overall statistics on cybercrimes and demonstrate the evolving nature of digital offenses. Kazakhstan's Criminal Code, dated July 3, 2014, No. 226-V [2], includes Chapter 7, which covers Articles 205-213 and addresses offenses in the fields of informatization and communications. This legal framework is crucial for prosecuting cybercrimes, although updates to strengthen penalties and address new forms of digital crime are necessary. The ongoing assessment of this legislation allows for improvements to keep pace with the evolving digital threats. As noted by Borisova et al. (2020), the current legal mechanisms require regular revisions to ensure effective protection against modern cyber threats [5]. Kazakhstan's cybersecurity efforts are reflected in initiatives like the "Digital Kazakhstan" program, which aims to enhance the country’s digital infrastructure and promote secure information systems. These programs have had a significant impact on reducing cybercrime rates, though challenges remain in terms of preventing and responding to new threats [3]. As Smirnov et al. (2018) highlights, the role of governmental programs is essential in curbing the rise of cybercrime, particularly in sectors involving sensitive personal data [4]. In the context of modern challenges in information security, it is essential to analyze the measures taken by law enforcement agencies to prevent and investigate criminal offenses in the field of information and communications. The Ministry of Internal

Affairs of the Republic of Kazakhstan has been actively implementing new technologies and methods to combat cybercrime. The integration of anti-fraud database systems with mobile operators, reducing the use of fake numbers, and blocking fraud calls are just a few steps in the direction of effective control over cyber threats [7]. As noted by Prokofiev et al. (2021), international cooperation in cybersecurity plays a crucial role in strengthening domestic efforts and improving overall defense against cybercrime [9]. In Kazakhstan, there has been successful cooperation between law enforcement agencies and cybersecurity companies. For instance, "Kaspersky Lab Central Asia" [7] actively participates in information exchange initiatives and joint events with law enforcement agencies, enhancing the overall cybersecurity in the region. This collaboration aligns with the findings of Ivanov and Petrova (2019), who emphasize the importance of such partnerships in mitigating cybercrime risks and enhancing national cybersecurity resilience [6]. Kazakh law enforcement agencies actively use various software and hardware tools to investigate and combat cybercrimes. For example, the XRY software suite is designed for extracting data from mobile devices and analyzing digital footprints, while network traffic analysis tools like Wireshark are used to study network attacks and detect potential cyber threats. Palantir software, which conducts comprehensive metadata analysis, is also utilized in cybercrime investigations, helping detect threats and prevent attacks [7]. This approach is consistent with the suggestions of Lebedev (2016), who advocates for the development of specialized tools and expertise in digital forensics to support investigations [10]. An overview of the current state of information and communications in Kazakhstan indicates a rapid increase in internet users, highlighting the active digitalization of society. According to the latest data from the digital hub Wunder Digital, 17.3 million people out of the 19.5 million population are internet users. Internet penetration stands at 89.2%, emphasizing the high level of digital literacy in the society. Google holds a leading position among search engines, with 83% of users preferring it. The distribution of the internet audience by regions is quite uniform, with the highest activity in the capital and

large cities. The internet user profile in Kazakhstan includes both genders, primarily aged between 20 and 41 years [1]. It is also worth noting that 88% of users access the internet daily, engaging in activities such as information searching, social media communication, shopping, and consuming various types of content. This overview not only highlights the high level of internet penetration but also the diversity of activities among users in the digital space, making the study of information and communications in the context of combating computer crimes and ensuring information security crucial.

Experimental Results. The survey results revealed interesting patterns regarding the frequency and types of cyber threats faced by individuals. Approximately 30% of respondents reported encountering cyber threats more than once a week, while 45% said they faced such threats at least once a month. Interestingly, 25% of the participants mentioned that they had not encountered any cyber threats in the past six months, indicating that the frequency of encounters varies widely among individuals (Fig. 1). When it comes to the most common types of cyber threats, phishing emerged as the leading concern, with 60% of respondents indicating they had experienced phishing attacks. These often involved fraudulent emails or websites designed to steal personal information. Another prevalent threat was fraud through malicious websites, which was reported by 50% of the participants. Additionally, 30% of respondents had encountered credit card fraud, and 20% experienced issues related to malware, such as viruses or spyware. These results highlight the widespread nature of cyber threats, with phishing and website fraud being the most commonly encountered forms. Given these findings, there is a clear demand for enhanced digital security tools, particularly those that could block phishing attempts and protect users from malicious websites.

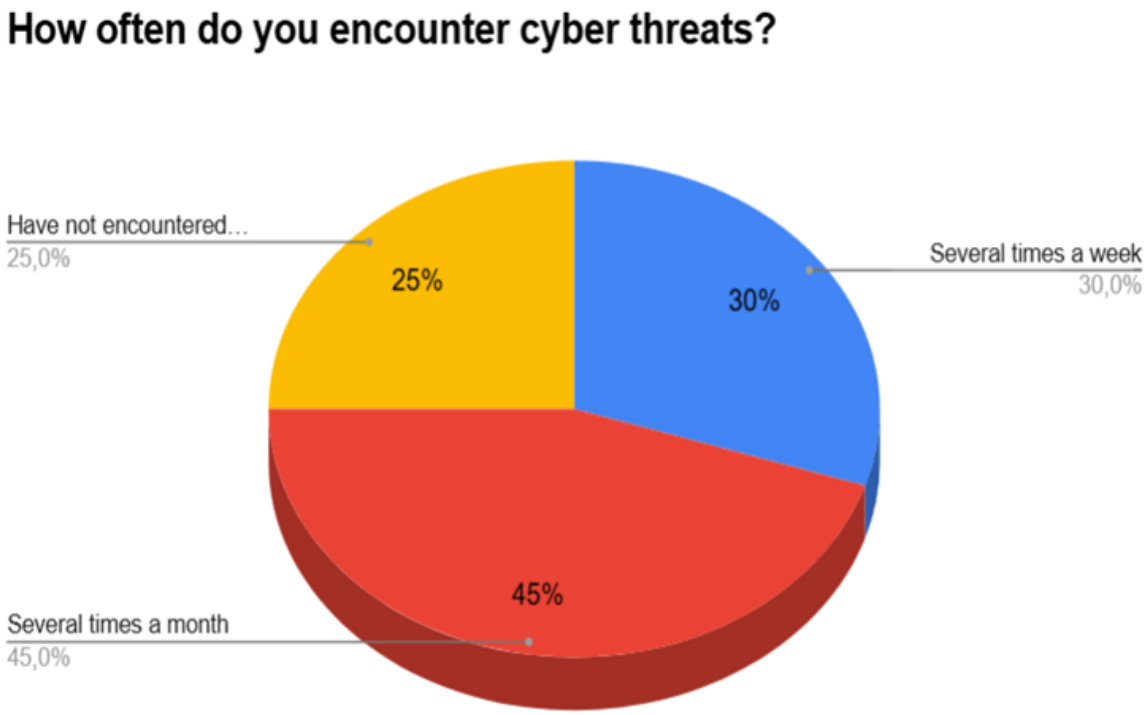

Fig.1. Survey Results (Question 1)

Conclusion. In conclusion, while Kazakhstan has made significant progress in addressing cybercrimes through legal reforms and cybersecurity programs, there is still a pressing need for further developments. Strengthening existing laws, improving enforcement mechanisms, and enhancing public-private collaboration are crucial steps in reducing cybercrime. Based on the analysis of data and survey results, it is evident that the two most common types of cyber threats are phishing (fraudulent emails and websites) at 60% and website fraud at 50%. Given these findings, the consideration of a platform or extension that, based on a database, would notify users about suspicious links, websites, and platforms presents a promising solution. This approach could be an effective way to mitigate the risks associated with these prevalent cyber threats and should be explored further.

References:

1. Wunder Digital. (2022). Digital Market of Kazakhstan: Trends, Risks, and Opportunities. https://wunder-digital.kz/digital-rynok-kazahstana-trendy-riski-vozmozhnosti/

2. Zakon.kz.(2014).Criminal Codeof Kazakhstan. https://online.zakon.kz/Document/?doc_id=31575252&sub_id=2050000&pos=3226;-54#pos=3226;-543

3. Digital Business. (2023). Internet Penetration in Kazakhstan. https://digitalbusiness.kz/2023-05-23/proniknovenie-interneta-v-kazahstane/

4. Smirnov, A. (2018). Cybercrime in Modern Society: Analysis and Trends. Information Security and Protection of Information, 3(25), 56-70.

5. Borisova, E.S. (2020). Technological Trends and Cyber Threats: Impact on Information System Security. Computer Security, 4(112), 34-48.

6. Ivanov, P., Petrova, M. (2019). Cybersecurity in the Modern Information Society: Challenges and Prospects. Journal of Cybersecurity, 2, 18-29.

7. Kaspersky Blog. https://blog.kaspersky.kz/

8. State Program "Digital Kazakhstan": Impact on the Development of Cybersecurity. (2018). Almaty, 82 p.

9. Prokofiev, A.B. (2021). International Cooperation in Cybersecurity: Experience and Prospects. International Law, 2, 88-102.

10. Lebedev, V.M. (2016). The Role of Education in Forming Personnel for Cybersecurity. Education and Science, 4(28), 76-89.