UDC 343.3/7:343.9
DOI: 10.32518/sals1.2024.221

Соціально-правові студії. 2024. Т. 7, № 1
Social & Legal Studios. 2024. Vol. 7, No. 1

Victimological aspects of countering internet crime: State and local government practices

Mamasaly Arstanbekov

PhD in Law, Associate Professor
Osh State University
723500, 331 Lenin Str., Osh, Kyrgyz Republic
https://orcid.org/0009-0001-1797-6427

Nurman Seidakmatov

PhD in Law, Doctoral Student
National Academy of Sciences of the Kyrgyz Republic
720071, 265A Chui Ave., Bishkek, Kyrgyz Republic
https://orcid.org/0009-0004-2261-4967

Marat Tatenov

PhD in Law, Associate Professor
Osh State University
723500, 331 Lenin Str., Osh, Kyrgyz Republic
https://orcid.org/0009-0008-7801-5022

Baktygul Kanybekova

PhD in Law, Associate Professor
Jusup Balasagyn Kyrgyz National University
720033, 547 Frunze Str., Bishkek, Kyrgyz Republic
https://orcid.org/0009-0006-3741-601X

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. Globalisation is a reason for increasing levels of anxiety, physical fatigue, and psychological problems, which weakens the ability of people to resist encroachment on themselves, especially in the Internet environment – the dominant sphere for communication. The study aims to identify the vectors of interaction between the state and potential victims of crime on the Internet by analysing the activities of the subjects of the direction in countries with different scientific and technical potentials. The study employed statistical methods to collect qualitative and quantitative indicators of the issue under consideration, as well as comparative analysis to compare the elements of state policy in the field of combating cybercrime. The intensity of crimes committed with the help of Internet tools is growing every year and it is primarily due to the growth of opportunities to perform various financial, social and other types of interaction in the online space. However, there is a direct correlation between the number of cybercrimes and the level of scientific and technological development of a country. According to the Global Innovation Index, some of the most innovatively developed countries are the United States of America, the United Kingdom and Japan, where the intensity of scientific progress is several times higher than in less developed countries, for example, in the Central Asian region. The role and place of state bodies concerning the prevention of Internet crime is extremely difficult to overestimate because it is the central and local government that has a leading position in the development of preventive measures to prevent and

Suggested Citation

Article's History: Received: 10.12.2023 Revised: 05.03.2024 Accepted: 28.03.2024

Arstanbekov, M., Seidakmatov, N., Tatenov, M., Kanybekova, B., & Kakeshov, B. (2024). Victimological aspects of countering internet crime: State and local government practices. *Social & Legal Studios*, 7(1), 221-234. doi: 10.32518/sals1.2024.221.

*Corresponding author

minimise the phenomenon of victimisation of society in the Internet space. The distinction and understanding of the types and directions of crimes in the online environment is necessary to create an effective mechanism to combat such crimes and to develop effective tools to inculcate a healthy lifestyle to prevent the development of victimisation traits in a person. The results of the work can be used as a practical basis for further research on the topic – development of state strategies to combat cybercrime

Keywords: collegial and one-man governance; human rights; scientific and technological capacity; collegial and one-man public authorities; hacker attacks; Global Innovation Index; countering Internet crime

Introduction

Although Internet crime has a history of about five to six decades, and in some countries less than that, it is a phenomenon that is of growing interest in society (Chadasama & Rajput, 2021). This is primarily because the implementation of this type of crime is most closely associated with the maximum involvement of ordinary citizens who are unsuspecting of their participation. Such citizens become unwitting accomplices of criminal actions, endangering not only themselves but also the state, its economic and social component, as well as creating challenges to the national security of the country. The topic of finding options for countering Internet crime through interaction between the population and government agencies is an urgent and timely issue. In the current context of the rapid growth of cybercrime and incidents involving the leakage of classified information of various defence establishments in some countries of the world, the victimological aspect of combating online crime is key. Awareness of ordinary Internet users and increasing their knowledge of safe behaviour on the Internet will be the basis for minimising the number of such incidents since in most cases ordinary citizens unknowingly pass on confidential information to criminals (Metelskyi & Kravchuk, 2023).

The issue of optimal ways to address cybercrime, organising preventive and preventive activities by government agencies and local self-government representatives, and educating the public on the basic rules and norms of interaction on the Internet has long existed. Much effort and attention has been devoted to its solution both by the official authorities and at the level of many public organisations. Therefore, it is essential to analyse in detail all components of modern state activity in the sphere of cyber defence and correctly prioritise the use of all mechanisms and tools in the fight against Internet crime, considering the victimological aspects of the sphere, since the security and successful development of the entire state depends on the training of the population and its mental readiness to resist online fraud.

The collapse of the Soviet Union and the rise of many young republics on the geopolitical map caused an immediate need to solve many problems, one of which was the topic of national security guarantees, in particular the protection of personal data and classified information. D. Aben (2019) believed that the main task of any government should be to react adequately to emerging problems that threaten national and regional stability and to take decisive steps regarding the most pressing problems. According to N.A. Seidakmatov and T. Narmamatova (2022), the media and all public personalities play a key role in the formation of a national strategy to protect the human right to privacy online. However, the authors did not consider the impact of ordinary citizens' careless behaviour on the frequency of online incidents to be a fundamental factor and root cause for the growth of cybercrime. Following M.U. Aliiaskarova (2022), the creation of a new world order emerged after the collapse of the bipolar security system. The researcher was the impetus for the formation of new structures and systems of global security, the basis of which on the border of the millennium became cyber activities and the development of online mechanisms to ensure stable and harmonious transformation of the state. However, the security of information arrays cannot be fully guaranteed, not so much because of the inherent victimisation of many Internet users, but because of the potential vulnerability of the online communication system itself.

The capabilities of new information technologies, such as artificial intelligence and innovative technical solutions, could be the basis for future cyber strategies in many countries around the world. H. Huang (2020) called these innovative tools – indispensable aids for relevant organisations and institutions dealing with Internet security issues – the most efficient and effective mechanisms for controlling and monitoring potential victims and, at the same time, unknowing co-conspirators of crimes committed on the Internet. D. Chudasama and N. Rajput (2021) and C.E. Griffith *et al.* (2023), on the contrary, believed that victimisation of society occurs precisely because of the large-scale application of information and communication technologies in all spheres of life and the context of collegial and sole management. Experts have identified restricting the free access of ordinary citizens to these technologies as the only way to slow the rate of cybercrime.

Public authorities, as a key source of control and execution of punitive functions, should act together with local government representatives to maximise the harmonisation of the communication process and improve the quality and speed of decision-making, which is particularly relevant for modern online interactions – both at the level of the individual and in the international arena (Sopilko & Rapatska, 2023). Local leadership, for example in individual states such as the USA or countries such as the UK, according to J.A. Hansen and G.L. Lory (2020), should take responsibility for educating the public on safe online behaviour. Furthermore, according to K. Yokotani and M. Takano (2021), intensive monitoring and control of citizens' interaction with social media and verification of content should be carried out by the representatives of the authorities – prosecutor's office, police – at the level of local government. At the same time, the ethical components of this issue are not discussed, as their consideration may lead to a weakening of control over citizens and, as a consequence, to a re-intensification of the processes of victimisation of society.

The study aims to identify the most effective areas of government action in the context of targeting potential and actual victims of cybercrime by examining and analysing various victimological aspects of the field in several countries around the world. The main objectives of the study are to identify the specifics of crimes committed in the Internet space; to identify the characteristic features and distinctive features of cybercrime counteraction in some countries of

the world; to summarise the factors that influence the choice of certain mechanisms and tools to minimise the victimisation of society.

Materials and methods

Scientific methods were used in the study to obtain a variety of practical information, generate data sets, draw conclusions and develop recommendations. The statistical method was used to analyse various qualitative and quantitative indicators related to cybersecurity, the fight against Internet crime and the prevention of online fraud in different countries. The method was also used to assess the performance of the development of scientific and technological potential of the world's states according to a comprehensive assessment of the innovation component of their economic and industrial development. The historical method was used to examine the stages of development of cybercrime policy in several countries by comparing periods and individual periods. In addition, the method was used to emphasise the differences in views and approaches to addressing the problem of internet crime in events such as the 2008 global economic crisis, the COVID-2019 coronavirus outbreak.

The comparison method was used to compare various indicators of some countries of the world in the context of analysing the effectiveness of their cybersecurity strategies through the prism of the general level of scientific potential. It was also used to evaluate different approaches to the application of certain steps in terms of the adequate response of central and local government officials to hacker attacks and breaches, using the example of such countries as the United States of America, South Korea, Great Britain. System analysis was used to identify general vectors and directions of research on the problem of cyber defence of personal data and classified information of the state and society in different countries of the world. System analysis was also used to fix the main subject of the work, its characteristics, specific features, common and distinctive features, functionality and dynamics of development in different periods.

The following materials were selected, reviewed and analysed to provide a more in-depth and effective consideration of the topic under study, namely the victimological components of combating online crime: Public Law No. 115-278 "Cybersecurity and Infrastructure Security Agency Act", 2018; state strategies and plans (Cybersecurity Strategy of the Kyrgyz Republic for 2019-2023, 2019; National Security Office, 2019; Cyber Security Strategy for Germany, 2021; HM Government, 2022; Office of National Security, 2023); statistical data (Zandt, 2023; Global Innovation Index, 2024; Internet World Stats, 2024); reports and reviews of international organisations and governmental authorities (9-48.000 – Computer Fraud and Abuse Act, 1986; Clark, 2023; Bundeskriminalamt, 2023); analytical material (Dzhumashova, 2021; Fixler & Furukawa, 2023; International Trade Administration, 2023). These materials supported the research presented here on countering Internet crime through the lens of assessing the potential of victimological aspects of public policy and contributed to the development of recommendations for further improving the interaction of all actors in the field.

Results

Basic concepts and terms for countering Internet crime. Countering and preventing Internet crime is currently a key topic of discussion at all levels of government and public administration in most countries, regardless of their level of scientific and technological development, which directly affects the range of options available to counter such crimes. According to several international organisations, statistics departments and cybercrime authorities in several countries (Cybersecurity Strategy of the..., 2019; Zandt, 2023; Fixler & Furukawa, 2023), cases of online extortion and financial fraud on the Internet have increased manifold over the last five years. This is especially true for such areas as so-called phishing (obtaining confidential data fraudulently) and money transfer fraud (during transactions, purchases) (Mikkola *et al.*, 2020; Seidakmatov & Narmamatova, 2022;) (Fig. 1). Since the involvement of outsiders, often unsuspecting citizens, in such crimes is maximised, national authorities must develop and effectively implement the components of civil self-control in the prevention of online crime.

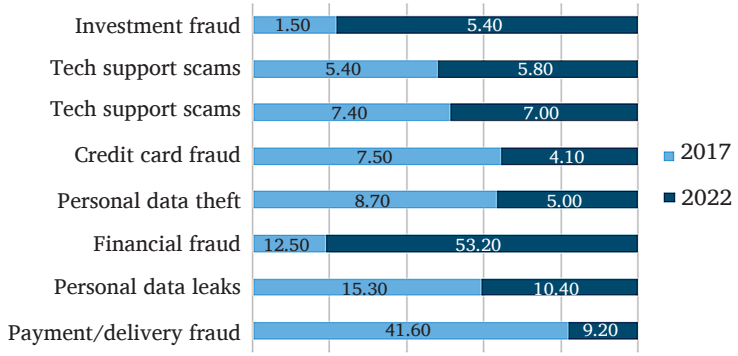

Figure 1. Percentage of the most common forms of cybercrime (comparison of 2017 and 2022 data, %)
Source: compiled by the authors based on G. Zandt (2023)

To better and more accurately analyse how cybercrime can be countered by assessing the various victimological aspects of cybercrime, it is important to first understand the basic terms and definitions of the topic. As such, according to some experts (Mikkola *et al.*, 2020; Aliiaskarova, 2022; Griffith *et al.*, 2023), the essence of the concept of "victimhood" includes a mental feature of a person or group of persons to increased susceptibility to the influence of others and, consequently, the property of often becoming a victim of crimes of different nature. Victimisation is the process (gradual or rapid) of transforming a person or group of persons into a victim or victims of such

crimes (Hawdon, 2021). Consequently, the victimological aspects of prevention in certain areas should be interpreted as activities aimed at prevention, prophylaxis, and skills training of individuals – potential or already accomplished victims of crime – to different types and levels of resistance to these crimes (Drew, 2020; Park *et al.*, 2022).

K. Yolotani and M. Takano (2021), M. Erendor and M. Yildirim (2022) believe that a distinction should be made between Internet crime, cybercrime and online crime, motivated by the fact that the Internet, as a global network, encompasses many concepts and components. Any action related to the technical, automated or machine aspects of the Internet can be considered cyber activity. Furthermore, online activity is exclusively related to real-time processes. However, although this distinction is used in the practical activities of several specialists, in this paper the concepts of Internet crime, cybercrime and online crime, as well as cyberterrorism (computer terrorism) will be used as synonyms.

Considering all Internet crimes in a generalised way, as a forensic manifestation of social attitudes, it is possible to define such crimes as any illegal actions involving a computer, server or network connection (Ismailova & Muhametjanova, 2016). Today, there are many different types of illegal actions and unauthorised transactions involving online tools. In 90% of cases, they target personal information (obtaining confidential data directly from the victim) – in such cases the amount of financial gain ranges from minimal to average, in the remaining 10% of cases – the crimes target organisations, businesses and other legal entities, causing substantial economic losses (Griffith *et al.*, 2023). All illegal cyber activities are carried out using a computer (less often a telephone) and local networks and servers, using a variety of techniques and schemes (Table 1).

Table 1. Types of cybercrime depending on the objectives and methods

Target	Cybercrime name	Crime aim
Humans	Replacement of email	E-mail distribution
	Spam	Advertisements
	Phishing*	Fake e-mail distribution
	Botnet**	Sending false instructions to other computers
	Net espionage	Hacking into individual computers for blackmail and extortion purposes
	Cyber defamation	Publishing untruthful information on websites or sending emails
	Espionage and/or cyberstalking	Sending e-mails, posting messages on bulletin boards, chat rooms, online user groups
Property	Credit card fraud	Obtaining a credit card number by illegal and/or fraudulent means
	Intellectual property offences	Software hacking, copying illegal software, illegal distribution of software copies
	Copyright infringement	Reproducing or performing a copyrighted product without proper authorisation
	Trademark infringements	Affiliation to a trademark without the authorisation of the trademark owner or licensees
Society	Forgery	Creation of fakes and dubplates (high and low quality) through the use of high-quality scanners, printers and computers
	Cyber-terrorism	Terrorist/hacker attacks on servers and online systems
	Clickjacking***	System and program hacks
Organisations	Digital bill theft	Banking system hacks
	Unauthorised access to a personal computer	Login and password cracking
	DoS attacks****	Executing various applications (spamming, spreading viruses) to disrupt network and/or server response
	Flooding	Virus/hacker attacks
	Digital “bombing”	Mass e-mail spam on one address
	“Logic” bomb	Running programs whose playback depends on events and/or algorithms
	Trojans	Unauthorised code execution within an authorised program by unauthorised subjects
	Data fraud	Execution of unauthorised commands

Note: * – gaining access to confidential user information; ** – a network of personal computers infected with viruses and malware; *** – a system of multiple exchange tasks performed on a website using malware to hack and obtain confidential information; **** – a hacker attack on a server and/or system to overload its infrastructure

Source: compiled by the authors based on H. Saleh *et al.* (2017), J. Hawdon (2021), J. Borwell *et al.* (2022), G. Zandt (2023)

The main goal of Internet fraud and various online offences is, first, to obtain financial gain through blackmail and extortion, and then (much less frequently) to inflict moral damage through the dissemination of untruthful confidential data or information of an intimate nature without the purpose of obtaining monetary reward (Lee & Wang, 2024). Specifically, regarding the harmful impact of cybercrime on various sectors of government development, it is worth highlighting the impact on business (financial and economic) and national defence (internal and external security).

Specific damages from the impact of hacking and hacker attacks on businesses and organisations around the world are difficult to quantify (Borwell *et al.*, 2022). Cybersecurity Ventures, an international organisation that assesses the

level of cybercrime in the world, estimates that online crime is growing at an annual rate of 15% and predicts that by 2025 the total damage from online crime could reach over $11 trillion (a preliminary estimate based on data from the world's largest businesses) (Oleksiewicz & Civelek, 2023).

The main and most harmful consequences for businesses and industries from online misconduct against them are: a drop in investor confidence as a response to poor protection of personal data (in case of hacker attacks); reduced flow of investments and capital expenditures, difficulties in raising additional capital; receiving fines and sanctions due to leaked personal data of clients (in case the situation escalates and the company is sued); reputational risks, which are among the most dangerous, as name and brand are now key signs of recognisability and popularity among customers; disruption of production processes, logistics routes and other elements of business and organisational operations due to hacking of web portals, servers or systems.

Hacker attacks can be even more dangerous to national security and state defence capabilities. Public health, banking and other areas that operate with massive amounts of personal data can be affected by unauthorised actions on their systems. Leaks of sensitive information can be catastrophic, especially if the information falls into the hands of terrorists, other criminal groups or competitors who can use the data at will, causing irreparable damage to the state and its citizens. Although the dynamics of cybercrime are becoming more intense every year, the level of identification of victims and attempts to assess the financial damage remains at a rather low level (Drew, 2020). This situation has many causes – overt and those that are hidden or tend to manifest themselves in the future. The causes can be grouped according to the following criteria (Chadasama & Rajput, 2021): access to personal data (refusal to provide information stored on personal electronic resources to law enforcement authorities); personal time (unwillingness to use time to visit the police to go through all the bureaucratic mechanisms – filing a report, drawing up an offence, giving evidence); interaction with law enforcement agencies (mistrust of representatives of the police, prosecutor's office and other agencies, based on various reasons); publicity risks (fear of publicity among acquaintances, colleagues, business partners about the situation, fear of criticism from their side); rights and freedoms awareness levels (low awareness of human rights in the sphere of online communications and rules of safe behaviour on the Internet).

Prevention and avoidance of any offence is the most important element in combating illegal actions. This is especially relevant in the context of Internet crimes, which are becoming a mass phenomenon in almost every country, in every sphere of state and public administration and are widely discussed by collegial and sole representatives of public authorities on most national and international platforms. At the moment, the level of prevention of this kind of atrocity remains unsatisfactory due to the uncontrolled growth in the number and directions of cybercrimes (Leukfeldt *et al.*, 2019). The main reason for this is the increase in the qualitative indicators of criminal acts committed when the dexterity and skill of fraudsters are higher than the same indicators of state representatives and responsible authorities. The peculiarity of such crimes is the maximum involvement of ordinary citizens (often without their knowledge and permission), so the activities to increase the level of education of the population to minimise the chances of growth of such phenomenon as victimhood in their environment, is one of the main goals of state and public policy (Wołyniec, 2018).

Victimological aspects to counter internet crime can be roughly divided into several areas (Tonellotto, 2019): legislative (development of appropriate legal and regulatory frameworks to improve the effectiveness and efficiency of the fight against cybercrime by working with victims of such offences); academic (intensification of scientific activity, expansion of the range of vectors of research work on the systematisation and classification of Internet crimes, their types, methods, specifics, peculiarities and other characteristic features); institutional (creation of structural subdivisions under state or local self-governance bodies or formation of independent structures or institutions to control, monitor, prevent and counteract crimes committed on the Internet); technical (launch of special software in enterprises or organisations, local implementation of innovative information and communication systems to protect against hacking and hacker attacks); ideological (fostering a culture of resistance to Internet crime in society by raising awareness of the importance of preventing such acts and participating in the fight against online criminals; education and awareness-raising activities among the population).

Combating cybercrime in different countries. Due to the ever-increasing number of cybercrime incidents, many governments have adopted proactive policies to prevent and counter such offences. A key feature of such actions is the extensive public participation and civic engagement in the processes of crime prevention and identification of attackers (Yokotani & Takano, 2021). This aspect of state-civil society interaction is crucial in the context of combating illegal activities on the Internet because ordinary citizens are often unknowingly and unknowingly complicit in such crimes.

Each state has its unique and innovative methods of combating online fraud. Some develop advanced systems and tools to identify criminals and carry out preventive measures (USA, European states (Notté *et al.*, 2021), while others use already proven inter-row experience (e.g., Central Asian countries) (Seidakmatov & Narmamatova, 2022). However, there is a direct correlation between the quantity and quality of ways and methods of countering Internet crime and the level of scientific and technological development in the state. Many experts in the field (programmers, sociologists, economists) note the following (Mikkola *et al.*, 2020; Borwell *et al.*, 2022): the higher the level of innovative development of the state, the more effective and qualitative it is in countering cybercrime (Table 2). But at the same time, it is more susceptible to these crimes due to the high concentration of various unique and sensitive information.

Table 2. Top countries by level of innovation development according to the Global Innovation Index, 2020-2023

Country	2023*	2022*	2021*	2020*
Switzerland	1 (67.6), 1	1 (64.6), 1	1 (65.5), 1	1 (66.08), 1
Sweden	2 (64.2), 3	3 (61.6), 2	2 (63.1), 2	2 (62.47), 2

Table 2, Continued

Country	2023*	2022*	2021*	2020*
United States of America	3 (63.5), 2	2 (61.8), 3	3 (61.3), 3	3 (60.56), 3
United Kingdom	4 (62.4), 7	4 (59.7), 8	4 (59.8), 10	4 (59.78), 9
Singapore	5 (61.5), 10	7 (57.3), 13	8 (57.8), 13	8 (56.61), 14
Finland	6 (61.2), 4	9 (56.9), 4	7 (58.4), 5	7 (57.02), 6
Netherlands	7 (60.4), 8	5 (58.0), 5	6 (58.6), 7	5 (58.76), 8
Germany	8 (58.8), 9	8 (57.2), 9	10 (57.3), 9	9 (56.55), 10
Denmark	9 (58.7), 12	10 (55.9), 12	9 (57.3), 14	6 (57.53), 12
South Korea	10 (58.6), 11	6 (57.8), 10	5 (59.3), 8	10 (56.11), 11
Kazakhstan	81 (26.7), 83	83 (24.7), 81	79 (28.6), 86	(56.11), 56
Uzbekistan	82 (26.2), 78	82 (25.3), 80	86 (27.4), 77	93 (24.54), 90
Kyrgyzstan	106 (20.2), 96	94 (21.1), 92	98 (24.5), 102	94 (24.51), 81
Tajikistan	111 (18.3), 85	104 (18.8), 84	103 (23.9), 80	109 (22.23), 77
Turkmenistan	**	**	**	**

Note: * – information for the year includes the following indicators: rank in the analysed year (total score), score for the level of knowledge & technology outputs; ** – no data available

Source: compiled by the authors based on Global Innovation Index (2024)

In the United States, which is one of the most technically advanced and innovative nations in terms of developing innovative solutions in various fields of production (3rd place among the world's countries in 2023, 2nd in 2022, 3rd in 2021 and 2020 (Global Innovation Index, 2024)), the issues of countering Internet terrorism are extremely important and high priority, as in the event of a hack, top-secret information and classified data may be leaked. The main document regulating relations in the sphere of countering various offences committed on the Internet or through online technologies is 9-48.000 – Computer Fraud and Abuse Act (1986). It is the main regulatory mechanism for preventing and combating Internet crime and describes all the different options and ways to counter and prevent it, including from a victimological perspective.

In terms of the organisation of Internet crime prevention activities, the US system is multifaceted and complementary, with many branches and different constituent structures (Mikkola *et al.*, 2020; Bjelajac & Filipović, 2021). There are several responsible bodies and units in the country, among which the key role at the state level is played by the US Department of Justice, under which there are several "subsidiary" structures that perform relevant functions at the local level in each state (Hansen & Lory, 2020). The Federal Bureau of Investigation has a special unit – Cybersecurity and Infrastructure Security Agency, created in 2018, which reports to the US Department of Homeland Security, which, in turn, considers cyberspace as one where crimes similar to those committed in real life are possible (Hawdon, 2021). CISA monitors and searches for cybercriminals monitors the Internet for new online threats and cyber fraud and provides information and services to protect the business sector and critical infrastructure from hacker attacks and unauthorised breaches of their defences (Public Law No. 115-278, 2018). There are also many other federal agencies and services operating in the United States, including United States Secret Service, whose main functions are to protect the president of the country, family members, real estate, and privacy on the Internet (in addition, the service is engaged in training local government officials in cyber literacy and the ability to counter cybercrime at the initial stage – namely, to conduct preventive work among the population; United States Immigration and Customs Enforcement, which combats illegal migration, human trafficking, sexual slavery, including through the use of online systems and Internet tools (Hawdon, 2021) and others.

At the local level, within the jurisdiction of individual state governments, there are various centres and organisations to combat internet crime (Public Law No. 115-278, 2018). The most widespread is the network of cybercrime centres, which consists of programmers and hacker groups searching for potentially dangerous Internet users. The activities of such centres are very productive because among their employees are specialists who were formerly cybercriminals but are now working for the state (Drew, 2020; Hawdon, 2021). This provides information on the nuances of online illicit activity and how to combat it. In addition, the state encourages the creation and development in every institution (organisations, firms, as well as schools, universities, kindergartens) of special cybersecurity control departments within the work of the individual enterprise. Thus, almost every enterprise employs specialists responsible for internal security in the online space and controlling the level of awareness of this danger among the employees of the organisation (Hawdon, 2021). This innovation has a crucial role to play when it comes to combating cybercrime in the country.

The basic principles and concepts of the direction, stipulated in the US regulatory framework, are presented in the Gramm-Leach-Bliley Act (GLBA) (1999) – on the rules of financial secrecy, which regulate the process of collection and disclosure of this information in a lawful way, as well as on security measures to minimise the chances of data leakage and dissemination of false information. Individual acts regulate activities in other areas of the online space and control decision-making processes regarding, for example, cyber blackmail, spam (Hawdon, 2021). The USA has a state-based practice of legislative activity at the level of individual states. For instance, the state of Massachusetts has adopted a special law that defines the concepts and physical boundaries of Internet offences and forms the number of fines and prison sentences for such offences exclusively within the state. Local authorities in the state of Tennessee define online harassment and ordinary harassment as the same action, accordingly, the punishment for it should also be identical and quite strict – a fine and arrest (depending on the severity of the offence) (Hansen & Lory, 2020).

The main areas of victimological prevention of Internet crime in the United States include an extremely high level of preventive action among the population, carried out both at the level of federal authorities and within individual states. This includes continuous training of both responsible employees and specialists in the field, as well as ordinary citizens, combating suspicious phenomena online, education of correct and cool behaviour in the process of online communications, filtering of any information and requests received from social networks, especially from strangers. For these purposes, society is taught to use all the possibilities of new information and communication technologies. Within the framework of cooperation between the countries of the European continent, until recently, no special efforts to jointly combat cybercrime were noted. Thus, at the beginning of the XXI century, the Council of Europe adopted the Convention on Cybercrime (2001); the Council of Europe Convention on the Prevention of Terrorism (2005), which includes provisions on various offences related to Internet activities; the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007); the Personal Data Protection Act (2008), which forms a list of unauthorised actions with personal information on the Internet and options of criminal punishment for these actions.

The aforementioned and other regulations have been applied with varying degrees of success by European countries in addressing cybercrime issues. However, since 2008, when the global economic crisis began, the protection of sensitive information, especially that related to financial and other personal data, was revealed to be a much stronger legislative basis for secrecy and other aspects of personal life. Therefore, since the beginning of the 10 years of the XXI century, European countries have been actively working together to develop new documents and regulations to combat Internet crimes. This activity reached its peak during the COVID-19 coronavirus outbreak, when almost all financial and social communication was transferred to the online sphere. Given the fact that the scientific potential of European countries remains at a very high level (for example, the UK has been ranked 4th among countries in the Global Innovation Index (2024) for the last 4 years, starting from 2020, while Germany was ranked 8th in 2023 and 2022, 10th in 2021 and 9th in 2020), the technical capabilities to fight cybercriminals are virtually unlimited, which allows for the involvement of a broad section of society in this process. Thus, amendments to the Regulation of the European Parliament and of the Council No. 2019/1020 "On Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU)" (2022) were made, including a list of actions mandatory for critical businesses to protect them from hacker attacks. The Act also amended the process of expanding the Internet infrastructure and regulating the rules of behaviour of different actors on the Internet (Oleksiewicz & Civelek, 2023).

The main document designed to increase the public's education on how to prevent victimisation in the online environment was the adoption of a Directive (EU) of the European Parliament and the Council No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (2022)", which introduces new principles and rules for the behaviour of businesses and companies, as well as individuals, on the Internet, and regulates the field of preventive and proactive work with the public in the context of combating online fraud. (Notté *et al.*, 2021; Button *et al.*, 2022). Besides policies at the pan-European level, there are also extensive efforts to combat Internet crime in individual states in the region.

The United Kingdom (UK) recognises the importance of combating cybercrime as it relates to national security, protection of citizens' rights, online freedom of expression, equality and openness. According to an independent study conducted by A. Clark (2023), every year since 2000, the number of businesses and individuals subjected to cyber-attacks has increased by 10-15% year-on-year. However, only 65% of businesses are aware that they have been subjected to fraud; the rest are unaware of it until the issue involves a significant financial loss. For instance, in 2016, a British hairdresser paid over £2,000 to online extortionists for the safety of its customers' data, while the outsourcing company Capita lost around £20 million in 2023 because its employees did not know the basic rules of online behaviour (e.g., writing down their logins and passwords for personal computers on paper and leaving them in a visible place at work or co-working rooms) (Wołyniec, 2018); Akdemir *et al.*, 2020). These and similar examples suggest that the level of education in terms of the rules of behaviour in the online environment in Britain is quite uneven and this causes serious material and image losses to the country, not to mention national security issues.

The Cabinet of Ministers (general areas of cybersecurity), the Department for Science, Innovation and Technology (implementation of legislative norms in the scientific and industrial environment), and the Ministry of Interior (monitoring and controlling potential Internet criminals) are all involved in Internet security issues (Sharma, 2020). At the level of local authorities, there are certain specialised centres for countering Internet crime (akin to similar centres in the US). The legislative field of the sphere in the UK is formed by several documents, the main and most comprehensive of which is the National Cyber Strategy (HM Government, 2022). The main objectives of the strategy are to formulate key tasks for the development of information technologies and online data protection in the coming years, to transform the country into a key fighter against Internet crime by 2030, to increase the level of citizens' education through constant open scientific events and practical training to minimise the victimisation processes of the British society, to optimise the cyber security structure by dividing responsibilities between state and local governments (Button *et al.*, 2022).

In Germany, the main responsibility for solving cybercrime lies with local authorities – prosecutors, police and other relevant institutions in the German states. For example, Bavaria has a successful Cyber Defence Platform, Hesse has a Cyber Competence Training Centre, and Cologne has a firm specialising in finding and catching dangerous hackers and internet fraudsters (Bundeskriminalamt, 2023). At the state level, the Bundeskriminalamt deals with Internet fraud, whose main tasks are to provide information on criminal cases of online crime, investigate cyberterrorism, and educate citizens about safe behaviour on the Internet (a separate unit within the agency, the Cybercrime Unit, is responsible for this) (Van de Weijer *et al.*, 2020). Following the example of other countries, Germany has a National Cy-

ber Defence Centre with many local cells in the federal states (Lee & Wang, 2024). The organisation collects and processes all kinds of information regarding the online activities of the population, searches for cybercriminals, provides information and services to legal entities and individuals regarding protection against hacker attacks. At the legislative level, Germany has adopted several acts that shape cyber policy in the country. Among the main ones is the Cyber Security Strategy for Germany (2021), which outlines the steps needed to secure the country's development and prevent the growth of Internet crimes involving ordinary Internet users. A key element of the document, which has been emphasised, is to increase the public's education and awareness of cybercrime and train them to protect themselves and their data at a basic and intermediate level of sophistication.

In the Asian region, Singapore, Japan, South Korea and others are among the leaders in terms of S&T development. The level of innovatization of the South Korean society allows us to talk about the country as one of the leaders in the region (South Korea's position according to the Global Innovation Index (2024): 10th place – in 2023 and 2020, 6th – in 2022, 5th – in 2021). The high level of technological progress makes the state extremely attractive for building and developing innovative businesses. At the same time, South Korea is the region's leader in the number of large-scale hacker attacks (International Trade Administration, 2023) (Table 3). Given its neighbourhood with North Korea, whose authorities are actively using the cyber component of terror against the South Korean population, Seoul's response is quite serious and productive.

Table 3. Cybercrime activity and characterisation of South Korean government counter-activity concerning incidents, 2000-2020

Year	Incident	Preventive measures	Legislative action (state level)
2000	–	Establishment of the Institute for National Security Studies (NSR)	–
2001	–	–	Adoption of the Law on the Protection of Information and Communication Infrastructure (PICI Law). Adoption of the Law on Electronic Government. Adoption of the Law on the Development of Information and Communication Networks. Adoption of the Law on the Use and Protection of Information
2003	Global Internet outage on 25 January	–	–
2004	–	Establishment of the National Cyber Security Centre (NCSC) within the National Intelligence Service (NIS)	Adoption of the National Crisis Management Core Directive. Establishment of a national cybercrisis management manual
2005	–	–	Adoption of the National Directive on Cyber Security Governance
2007	–	–	Amendments to the Law on Electronic Government
2009	DDoS attack on 7 July	Implementation of a national integrated response to cybercrisis	–
2010		Initiation of the cyber command structure under the Ministry of Internal Affairs	Amendments to the Law on Electronic Government
2011	DDoS attack on 4 March. Hacking into the security systems of NH Bank, a financial institution, on 4 March	Development of a National Cybersecurity Master Plan	–
2012	–	Establishment of a joint public-private and military cyberspace. Establishment of a cyber-threat response team	–
2013	Cyberattack on 20 March. Cyberattack on 25 March	Launch of a comprehensive national cybersecurity programme	–
2014	Launch of a comprehensive national cybersecurity programme	Establishment of the Cyber Security Training and Education Centre (CSTEC) at the National Intelligence Service (NIS)	–
2015	–	Appointment of a cybersecurity advisor in the Presidential Administration. Establishment of the Financial Security Institute (FSI). Adoption of measures to raise the national cybersecurity profile of the state	Adoption of the Law on the Development of the Cyber Security Industry
2016	Interpark e-commerce service hack	K-ICT convergence security strategy	–
2017	WannaCry ransomware attack. Nayana ransomware attack	–	–

Table 3, Continued

Year	Incident	Preventive measures	Legislative action (state level)
2018	North Korean hacking attack on security during the Olympics	–	–
2019	–	National Cybersecurity Strategy. National Cybersecurity Baseline Plan	–
2020	–	–	Amendments to the National Intelligence Service Act

Source: compiled by the authors based on National Security Office (2019), S.J. Kim and S. Bae (2021), K. Yokotani and M. Takano (2021), International Trade Administration (2023)

The key actors and their basic functions are outlined in several South Korean regulations, one of the most comprehensive and extensive of which is the Yoon Suk Yeol Administration's National Security Strategy (Office of National Security, 2023). The document thoroughly analyses the current state of cyber defence in the Republic, forms the main objectives (content monitoring, search for potential threats, eliminating the danger, dealing with the consequences), large-scale informing of the population about the threats of online communication, and so on. The Yoon Suk Yeol Administration's National Security Strategy (Office of National Security, 2023) also talks about strengthening international cooperation in this area, especially with the United States.

According to certain Asian and South Korean experts (Jaishankar, 2020; Yokotani & Takano, 2021; Park *et al.*, 2022), Seoul-Washington cooperation on Internet crime issues is an example to follow around the world. The number and quality of agreements signed, and the size and scope of joint activities conducted by the two countries suggest a deep level of cooperation. For example, the Strategic Cybersecurity Cooperation Framework between the Republic of Korea and the United States of America (2023) was signed, according to which the parties committed to jointly develop cyberinfrastructure, create a safe Internet space, share experience and information, and educate the population on Internet literacy. As Washington's main partner in Asia, Seoul also utilises the positive experience of the United States in the context of engaging with the public on cybercrime prevention. Internet crime prevention centres have been established in the country, and many activities are held each year to increase the online security literacy of South Korean society (Fixler & Furukawa, 2023). However, unlike the United States, in the Republic, the local government is not as autonomous in cybersecurity and ensuring the protection of national interests. Therefore, the central government has a key role in countering unauthorised acts on the Internet through the implementation of state acts, strategies and plans.

In Kazakhstan, Uzbekistan, Kyrgyzstan, Turkmenistan and Tajikistan, it is currently difficult to provide a definitive answer regarding the level of cyber defence of their government agencies and financial and economic institutions. At the national level, there are various bodies (state and private-public actors) whose main tasks are to carry out actions aimed at combating Internet crime. However, the most productive are the results of working together with international organisations through various initiatives (Tonellotto, 2019; Huang, 2020;). An example of such cooperation is a project of the Organisation for Security and Co-operation in Europe (OSCE) to intensify the scientific and educational capacity of five Central Asian states to support the sustainable development of the Internet space and successfully counter cybercrime (Erendor & Yildirim, 2022; Kakeshov *et al.*, 2023). The project consists of several phases: an initial assessment of the countries' scientific and technological capabilities and the level of training for cybersecurity professionals, training to improve the skills of these professionals and increase general computer literacy, and the development of training programmes for civilians in conjunction with trained experts from the region.

Following A. Dzhumashova (2021), as of 2021, every fourth Internet user in the country has experienced cyber fraud. Given the heterogeneous level of Internet penetration in the region (Table 4), it is possible to state that in some areas this indicator may be higher.

Table 4. Internet crime rate in Central Asian countries as of 2022

Country	Population	Number of Internet users (% of total population)
Kazakhstan	19,146,252	16,465,777 (76.6)
Uzbekistan	34,271,815	17,161,534 (50.1)
Kyrgyzstan	6,703,015	3,683,700 (55)
Tajikistan	9,898,203	3,013,256 (30.4)
Turkmenistan	6,177,955	1,562,794 (25.3)

Source: compiled by the authors based on D. Aben (2019), Internet World Stats (2024)

Due to the increasing pace of the spread of Internet technologies and the growing number of active Internet users as potential victims of cyberfraud and unwitting accomplices of online crimes, cooperation in the area of cyber security with international players such as the OSCE, the United Nations, the European Union and others is crucial for Kyrgyzstan in the context of using positive experience and implementation of certain normative legal acts, as well as norms and standards into national practice.

Considering some examples of countering cybercrime in several countries with different levels of innovative development, it can be concluded that, regardless of the level of scientific and technological capacity, every state can become a victim of offences committed with the help of online tools. However, the frequency and intensity of these crimes directly depend on the level of training and general awareness of the population about the rules of safe behaviour on the Internet. The victimisation component of a country's

cybercrime strategy is extremely important and is key to guaranteeing the security of national borders and sensitive data. Analysing the results obtained the study and analysis the specifics of policies to counter Internet crime in countries with different levels of scientific and technological capacity, it is possible to state that these countries have both common problems and their specific features and nuances. In general, several groups of general recommendations for improving the quality of interaction between actors in the field of cybercrime prevention and combating cybercrime can be suggested.

For public authorities in the legislative sector, the following should be done: develop or update national cyber security strategies to adequately respond to contemporary threats; establish a budgetary programme for equitable and fair financing of the sphere; involve international partners in the process of drafting regulations, thus strengthening cooperation with them; strengthen inter-agency cooperation within the country. Responsible officials and supervisory bodies in the sphere at the level of local authorities should be identified in the institutional sector.

Local governments should intensify research and development activities in educational institutions, and scientific organisations under their jurisdiction (academic sector); update software to minimise the occurrence of cyber-attacks and to make it easy to use all means of protection against them (technical sector); organise and conduct information events (seminars, webinars, round tables) on the opportunities and prospects of countering Internet fraud for every citizen, creating a sense of duty and responsibility in society for their behaviour in the online space (in the ideological sector).

Discussion

Studying the issues of victimological aspects of countering Internet crime in the context of analysing the activities of state authorities and representatives of local self-government, namely, what steps are taken by the country's officials to minimise the frequency of incidents related to Internet crime, some conclusions were summarised. The topic of reducing the level of victimisation processes in society by raising general awareness and teaching the rules of behaviour on the Internet, as well as through the notion and awareness of elementary preventive steps against cyber fraudsters, is extremely relevant and widely discussed at all levels of government and public control. Considering the results and conclusions of research of specialists in the field – programmers, economists, sociologists, criminologists – the following can be summarised: interest in the problem of cyber defence of the country, its financial and banking sectors, protection of personal data has increased significantly in recent decades, and this is primarily due to the rapid spread of information and communication technologies. The demand for scientific research on this topic is high, and the results of this work will determine the further development of strategies for the protection of information on the Internet, especially those related to the components of national security. Experts from Central Asian countries, Kyrgyzstan and Kazakhstan, have focused their work on the specifics of government policy on cyber activities in the region and looked at the global experience through the prism of using it to minimise the increase in victimisation. Researchers from other countries (USA, Poland, Italy) focused on analysing national strategies and plans to protect information systems from potential hacking and explored ways to engage their citizens in these activities. To summarise, it is possible to conclude that the key theses of the researchers speak in favour of the fact that shortly the situation in the sphere of cyber security will be dynamically developing, creating new threats to the national security of individual countries and their citizens, as well as entire regions. Therefore, to adequately respond to these threats, it is necessary to act together, harmoniously combining activities at all levels of collegial and sole management, creating a synergistic interaction between the citizen and the country to protect their confidential data.

The paper voiced the opinion that in the late XX century – early XXI century there was a rapid intensification of the processes of informatisation of society and the spread of information and communication technologies through the widespread use of computers, mobile applications and the Internet has become an unprecedented phenomenon in world history. J. Hawdon (2021) shares similar opinions, calling the invention of the Internet a turning point in the history of mankind, and the rapid spread of e-mail technologies, social messengers, web resources and streaming services a unique example of revolutionary transformation and the transition of mankind to a new level of development. At the same time, the author was sure that in the event of the disappearance of these technologies, which have already become part of modern man's life, nothing fundamentally catastrophic could happen, except for the long-term inconvenience of ordinary citizens due to the lack of their usual means of communication.

Online crime factors such as the transmission of massive amounts of sensitive information and access to confidential data are the reasons why the vast majority of cybercrime is committed, as identified in this paper. K. Jaishankar (2020) also agreed with this, in whose opinion Internet blackmail, online extortion and other similar illegal actions are the main types of Internet crimes and for which the perpetrators should be seriously punished. At the same time, the expert expressed doubts about the appropriateness of further singling out cybercrime as an atrocity, explaining that the same offences are committed in real life without the use of computer technology.

The increased victimisation of society, regardless of the country, its level of economic and political development, and the quality of its scientific and technological capabilities, is a key factor shaping the extent of cybercrime for that state (Hasanova *et al.*, 2023). This idea voiced in the paper was also considered a fair statement by S. Park *et al.* (2022), who believed that today, to develop adequate strategies for the development of cyber security policy of the state, it is necessary to address the human factor and its impact on all spheres of activity of collegial and sole representatives of public authorities without exception. When considering the situation in South Korea, the experts argued that in this case the level of interaction between society and the government is maximised and the vulnerability of individuals to computer crimes is minimal, precisely because of the thorough and verified preventive activities of government agencies.

The essence of the influence of criminal methods on the individual in the context of increasing personal susceptibility to victimisation lies in many factors, among which are: the need for communication, the desire to exchange interesting information, the search for new acquaintances and the establishment of friendly or professional ties (Saliu *et*

al., 2022). R. Notté *et al.* (2021) share the opinion, calling such human desires the reason for the intensification of Internet crime in the 21st century and the main factor contributing to the active actions of cybercriminals, who exploit the human tendency to unknowingly commit illegal acts for their criminal purposes. Although the authors were confident that, through carefully designed policies and the joint efforts of central and local authorities, the victimisation of the population could be mitigated and thus Internet crime could be minimised.

The aspect of state involvement in addressing the protection of citizens and their data on the Internet was identified in the presented work as an important and indispensable condition in the fight against cybercrime. C.S. Lee and Y. Wang (2024) also referred to the synergy between the country's governing bodies of different levels of influence – central and local – as a key foundation for the prevention of unauthorised activities on online platforms. At the same time, however, the authors argued that it is not necessary to initially separate victims and perpetrators, as the state itself may, through its rash and harsh decisions, incite potential victims of crime to assist perpetrators, already consciously.

In the process of studying the topic of formation and development of policy in the field of cyber defence and protection of personal data on the Internet through, among other things, active involvement of the population in preventive and proactive processes in this area, some aspects have been identified. Analysing the vectors of research and the conclusions of scientists based on their scientific studies, it is possible to conclude that worldwide interest in obtaining detailed information on the subject under study, especially in the context of preventive measures of cyber data protection, is high. The main factor that makes the state authorities deal with data protection issues in the online sphere is the risk of leakage not only of personal content of ordinary citizens but also the loss of sensitive information of an economic or political nature (Rafalskyi, 2023). Therefore, most countries have recognised this problem and have identified areas that need to be urgently addressed. This includes minimising the victimisation of the population by using all opportunities and mechanisms available to accomplish this task. Because countries have different levels of scientific and technological potential and the development of advanced technologies is uneven, it is possible to state that the level of innovation of society depends on the intensity of hacker attacks against the state. At the same time, the lower the level of education of the population in terms of information and communication technologies, the higher the probability of the inability of such a country to adequately respond to online crimes against them (Horoshko *et al.*, 2021). Identification of key components, possible directions and vectors of development of the sphere of cyber protection of state data is an essential condition for the harmonious development of the country and its citizens, formation of a national security strategy taking into account all possible challenges and threats with maximum participation of civil society to minimise victimisation processes among its most vulnerable members.

Conclusions

Studying the characteristics and specifics of countering Internet crime in countries with different levels of scientific and technological development through the prism of analysing the likelihood of the impact of the victimisation characteristics of civil society on these crimes, some conclusions were made. It was found that the problem of the relationship between the psychological characteristics of a person unconsciously falling under the influence of attackers and the dynamics of growth of illegal actions with their help does exist, and this problem became especially relevant in the early XXI century when the population began to increasingly use the tools of the Internet, communicating through social networks and online messengers.

The level of scientific and technological progress of the state was identified in the study as one of the key factors contributing to a more effective fight of this state against cyber criminals and for very effective preventive and educational work with the population to increase their level of education and understanding of the rules of safe behaviour on the Internet. At the same time, the high level of innovation in sectors of government such as the economy, social services, banking and finance makes them desirable targets for Internet fraudsters, as the high level of digitalisation and informatisation of these areas means that all critical information is gathered in one place and stored in a single array, making it easier to steal.

In recent decades, starting from the late 1990s, the number of offences committed with the help of online tools has increased manifold. This fact is confirmed by the fact that during this period the volumes of financial losses of large enterprises and corporations amount to billions of dollars, although at the end of the twentieth century, the scale of economic losses was much smaller. The main reason for this situation is insufficient preparation of the population for this type of incident and the low level of general computer education in the sphere of self-protection and safe behaviour on various services on the Internet.

Minimising victimological processes in society, educating the population to adequately respond to suspicious actions in cyberspace, and the ability to protect their data in the online environment are key objectives in most strategies and plans for the development of cyber defence of the state and its interests. An important condition for the achievement of these goals is harmonious cooperation between the central government and local government representatives in the context of reasonable division of responsibilities, planning of joint activities, monitoring and timely identification of threats and dangerous trends. However, the future development of the sphere of countering Internet crime remains uncertain due to the unstable situation in the modern geopolitical space and the lack of a stable psychological basis for the healthy development of states and societies in them.

To provide a more accurate and thorough analysis of the specifics of combating Internet crime, to develop mechanisms to minimise the victimisation of society and to improve the quality of the results obtained, a study of the methods of combating illegal cyber activities in Central Asian countries in the context of comparing the policies of their government agencies seems appropriate for the next research.

Acknowledgements

None.

Conflict of interest

None.

References

[1] 9-48.000 – Computer Fraud and Abuse Act. (1986, September). Retrieved from https://www.justice.gov/jm/jm-9-48000-computer-fraud.

[2] Aben, D. (2019). Regional security in Central Asia: Addressing existing and potential threats and challenges. *Eurasian Research Journal*, 1(1), 51-65.

[3] Akdemir, N., Sungur, B., & Başaranel, B. (2020). Examining the challenges of policing economic cybercrime in the UK. *Journal of Security Sciences, International Security Congress (Special Issue)*, 113-134. doi: 10.28956/gbd.695956.

[4] Aliiaskarova, M.U. (2022). Classification of threats to personal information security. *Bulletin of KRSU*, 22(7), 64-69. doi: 10.36979/1694-500X-2022-22-7-64-69.

[5] Bjelajac, Ž., & Filipović, A. (2021). Specific characteristics of digital violence and digital crime. *Law – Theory and Practice*, 38(4), 16-32. doi: 10.5937/ptp2104016B.

[6] Borwell, J., Jansen, J., & Stol, W. (2022). The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory. *Social Science Computer Review*, 40(4), 933-954. doi: 10.1177/0894439320983828.

[7] Bundeskriminalamt. (2023). *Cybercrime*. Retrieved from https://www.bka.de/EN/OurTasks/AreasOfCrime/Cybercrime/cybercrime_node.html.

[8] Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., Kapend, R., & Wang, V. (2022). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. *Criminology & Criminal Justice*. doi: 10.1177/17488958221128128.

[9] Chadasama, D., & Rajput, N. (2021). Protecting ourselves from digital crimes. *National Journal of Cyber Security Law*, 4(1), 1-6.

[10] Clark, A. (2023). *Cybersecurity in the UK*. Retrieved from https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf.

[11] Convention on Cybercrime. (2001, November). Retrieved from https://rm.coe.int/1680081561.

[12] Council of Europe Convention on the Prevention of Terrorism. (2005, May). Retrieved from https://rm.coe.int/16808c3f55.

[13] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. (2007, October). Retrieved from https://rm.coe.int/1680084822.

[14] Cyber Security Strategy for Germany. (2021, October). Retrieved from https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf.

[15] Cybersecurity Strategy of the Kyrgyz Republic for 2019-2023. (2019, July). Retrieved from https://cbd.minjust.gov.kg/15479/edition/962966/ru.

[16] Directive (EU) of the European Parliament and of the Council No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)". (2022, December). Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2555.

[17] Drew, J. (2020). A study of cybercrime victimisation and prevention: Exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, 6(1), 17-33. doi: 10.1108/JCRPP-12-2019-0070.

[18] Dzhumashova, A. (2021). *Every fourth internet user faces cyber threats in Kyrgyzstan*. Retrieved from https://24.kg/obschestvo/206804_vkyirgyizstane_kajdyiy_chetvertyiy_polzovatel_interneta_stolknulsya_skiberugrozami/.

[19] Erendor, M., & Yildirim, M. (2022). Cybersecurity awareness in online education: A case study analysis. *IEEE Access*, 10(4), 52319-52335. doi: 10.1109/ACCESS.2022.3171829.

[20] Fixler, A., & Furukawa, S. (2023). *U.S.-South Korean cyber cooperation can combat North Korean threats*. Retrieved from https://www.fdd.org/analysis/2023/06/26/us-south-korean-cyber-cooperation-can-combat-north-korean-threats/.

[21] Global Innovation Index. (2024). Retrieved from https://www.wipo.int/global_innovation_index/en/.

[22] Gramm-Leach-Bliley Act (GLBA). (1999, November). Retrieved from https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.

[23] Griffith, C.E., Tetzlaff-Bemiller, M., & Hunter, L.Y. (2023). Understanding the cyber-victimization of young people: A test of routine activities theory. *Telematics and Informatics Reports*, 9, article number 100042. doi: 10.1016/j.teler.2023.100042.

[24] Hansen, J.A., & Lory, G.L. (2020). Rural victimization and policing during the COVID-19 pandemic. *American Journal of Criminal Justice*, 45(4), 731-742. doi: 10.1007/s12103-020-09554-0.

[25] Hasanova, J.V., Najafova, K.A., & Dilyard, J.R. (2023). Changed e-commerce behaviors of Azerbaijani consumers during the pandemic period. *Journal of Eastern European and Central Asian Research*, 10(7), 977-988. doi: 10.15549/jeecar.v10i7.1287.

[26] Hawdon, J. (2021). Cybercrime: Victimization, perpetration, and techniques. *American Journal of Criminal Justice*, 46(6), 837-842. doi: 10.1007/s12103-021-09652-7.

[27] HM Government. (2022). *National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK*. Retrieved from https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022.

[28] Horoshko, O.-I., Horoshko, A., Bilyuga, S., & Horoshko, V. (2021). Theoretical and methodological bases of the study of the iimpact of digital economy on world policy in 21 century. *Technological Forecasting and Social Change*, 166, article number 120640. doi: 10.1016/j.techfore.2021.120640.

[29] Huang, H. (2020). Analysis on the criminal subject of artificial intelligence. In *Data processing techniques and applications for cyber-physical systems (DPTA 2019)* (pp. 317-321). Singapore: Springer. doi: 10.1007/978-981-15-1468-5_40.

[30] International Trade Administration. (2023). *South Korea Cybersecurity*. Retrieved from https://www.trade.gov/market-intelligence/south-korea-cybersecurity.

[31] Internet World Stats. (2024). *Asia: Asia marketing research, internet usage, population statistics and Facebook subscribers*. Retrieved from https://www.internetworldstats.com/asia.htm.

[32] Ismailova, R., & Muhametjanova, G. (2016). Cyber crime risk awareness in Kyrgyz Republic. *Information Security Journal: A Global Perspective*, 25(1-3), 32-38. doi: 10.1080/19393555.2015.1132800.

[33] Jaishankar, K. (2020). Cyber victimology: A new sub-discipline of the twenty-first century victimology. In *An international perspective on contemporary developments in victimology: A festschrift in honor of Marc Groenhuijsen* (pp. 3-19). Cham: Springer. doi: 10.1007/978-3-030-41622-5_1.

[34] Kakeshov, B.D., Kanybekova, B.K., Seidakmatov, N.A., Zheenalieva, A.O., & Kokoeva, A.M. (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, 987-993. doi: 10.46852/0424-2513.2s.2023.48.

[35] Kim, S.J., & Bae, S. (2021). Korean policies of cybersecurity and data resilience. In *The Korean way with data. How the world's most wired country is forging a third way* (pp. 39-60). Washington: Carnegie Endowment for International Peace.

[36] Lee, C.S., & Wang, Y. (2024). Typology of cybercrime victimization in Europe: A multilevel latent class analysis. *Crime & Delinquency*, 70(4), 1196-1223. doi: 10.1177/00111287221118880.

[37] Leukfeldt, E.R., Notté, R.J., & Malsch, M. (2019). Exploring the needs of victims of cyber-dependent and cyber-enabled crimes. *Victims & Offenders*, 15(1), 60-77. doi: 10.1080/15564886.2019.1672229.

[38] Metelskyi, I., & Kravchuk, M. (2023). Features of cybercrime and its prevalence in Ukraine. *Law, Policy and Security*, 1(1), 18-25.

[39] Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B.L., Savolainen, I., Sirola, A., Zych, I., & Paek, H.-J. (2020). Situational and individual risk factors for cybercrime victimization in a cross-national context. *International Journal of Offender Therapy and Comparative Criminology*. doi: 10.1177/0306624X20981041.

[40] National Security Office. (2019). *National Cybersecurity Strategy*. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National Strategies Repository/National%20Cybersecurity%20Strategy South%20Korea.pdf.

[41] Notté, R., Leukfeldt, E.R., & Malsch, M. (2021). Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. *International Review of Victimology*, 27(3), 272-294. doi: 10.1177/02697580211010692.

[42] Office of National Security. (2023). *The Yoon Suk Yeol administration's National Security Strategy: Global pivotal state for freedom, peace, and prosperity*. Retrieved from https://overseas.mofa.go.kr/viewer/skin/doc.html?fn=20230621040037933.pdf&rs=/viewer/result/202403.

[43] Oleksiewicz, I., & Civelek, M.E. (2023). Where are the changes in EU cybersecurity legislation leading? *Humanities and Social Sciences*, 30(4), 183-197. doi: 10.7862/rz.2023.hss.50.

[44] Park, S., Lim, J., & Kim, D. (2022). The human factor of cybersecurity and the prevention and counter measures against cybercrime in South Korea. *Webology*, 19(2), 7962-7976.

[45] Personal Data Protection Act. (2008, January). Retrieved from https://www.informatica-juridica.com/anexos/personal-data-protection-act-2008/.

[46] Public Law of United States of America No. 115-278 "Cybersecurity and Infrastructure Security Agency Act". (2018, November). Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/3359.

[47] Rafalskyi, M. (2023). Offences in the sphere of virtual assets turnover and analysis of their qualification. *Law Journal of the National Academy of Internal Affairs*, 13(3), 65-76. doi: 10.56215/naia-chasopis/3.2023.65.

[48] Regulation of the European Parliament and of the Council No. 2019/1020 "On Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU)". (2022, September). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454.

[49] Saleh, H., Rezk, A., & Barakat, S. (2017). The impact of cyber crime on e-commerce. *International Journal of Intelligent Computing and Information Sciences*, 17(3), 85-96. doi: 10.21608/ijicis.2017.30055.

[50] Saliu, H., Rexhepi, Z., Shatri, S., & Kamberi, M. (2022). Experiences with and risks of internet use among children in Kosovo. *Journal of Elementary Education*, 15(2), 145-164. doi: 10.18690/rei.15.2.145-164.2022.

[51] Seidakmatov, N.A., & Narmamatova, T. (2022). The role of mass media in ensuring information security of Kyrgyz Republic. *News of the National Academy of Sciences of the Kyrgyz Republic*, 4, 156-164.

[52] Sharma, R. (2020). Legislation related to cyber crimes in United Kingdom. *Bournemouth University*. doi: 10.13140/RG.2.2.28198.34885.

[53] Sopilko, I., & Rapatska, L. (2023). Social-legal foundations of information security of the state, society and individual in Ukraine. *Scientific Journal of the National Academy of Internal Affairs*, 28(1), 44-54. doi: 10.56215/naia-herald/1.2023.44.

[54] Strategic Cybersecurity Cooperation Framework between the Republic of Korea and the United States of America. (2023, April). Retrieved from https://www.president.go.kr/download/644956452f9e3.

[55] Tonellotto, M. (2019). Crime and victimization in cyberspace: A socio-criminological approach to cybercrime. In *Handbook of research on trends and issues in crime prevention, rehabilitation, and victim support* (pp. 248-264). Hershey: IGI Global. doi: 10.4018/978-1-7998-1286-9.ch014.

[56] Van de Weijer, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: Determinants, motives, and previous experiences. *Policing: An International Journal of Police Strategies & Management*, 43(1), 17-34. doi: 10.1108/PIJPSM-07-2019-0122.

[57] Wołyniec, J. (2018). The UK government's response to cyber threats. *Teka of Political Science and International Relations*, 13(2), 143-154. doi: 10.17951/teka.2018.13.2.143-154.

[58] Yokotani, K., & Takano, M. (2021). Social contagion of cyberbullying via online perpetrator and victim networks. *Computers in Human Behavior*, 119, article number 106719. doi: 10.1016/j.chb.2021.106719.

[59] Zandt, G. (2023). *The most prevalent forms of cyber crime*. Retrieved from https://www.statista.com/chart/30870/share-of-worldwide-cyber-attacks-by-type/.

Віктимологічні аспекти протидії інтернет-злочинності: діяльність державних органів влади та місцевого самоврядування

Мамасали Сарбашович Арстанбеков

Кандидат юридичних наук, доцент
Ошський державний університет
723500, вул. Леніна, 331, м. Ош, Киргизька Республіка
https://orcid.org/0009-0001-1797-6427

Нурман Адісович Сейдакматов

Кандидат юридичних наук, докторант
Національна академія наук Киргизької Республіки
720071, просп. Чуй, 265А, м. Бішкек, Киргизька Республіка
https://orcid.org/0009-0004-2261-4967

Марат Бейшенбекович Татенов

Кандидат юридичних наук, доцент
Ошський державний університет
723500, вул. Леніна, 331, м. Ош, Киргизька Республіка
https://orcid.org/0009-0008-7801-5022

Бактигуль Канибуківна Канибекова

Кандидат юридичних наук, доцент
Киргизький національний університет імені Жусупа Баласагына
720033, вул. Фрунзе, 547, м. Бішкек, Киргизька Республіка
https://orcid.org/0009-0006-3741-601X

Бакыт Дайрабайович Какешов

Кандидат юридичних наук, доцент
Киргизький національний університет імені Жусупа Баласагына
720033, вул. Фрунзе, 547, м. Бішкек, Киргизька Республіка
https://orcid.org/0000-0003-1570-1072

Анотація. Глобалізація є причиною зростання рівня тривожності, фізичної втоми, психологічних проблем, що послаблює можливості людини протистояти посяганням на себе, особливо, в інтернет-середовищі – домінуючій сфері для комунікації. Мета полягає в окресленні векторів взаємодії держави та потенційних жертв злочинів в Інтернеті шляхом аналізу діяльності суб'єктів напряму в країнах із різним науково-технічним потенціалом. Методами дослідження були статистичний, за допомогою якого зібрано якісні та кількісні показники розглядуваного питання, та порівняльний аналіз, використовуючи який зіставлено елементи державної політики у сфері протидії кіберзлочинності. Інтенсивність злочинів, скоєних за допомогою інтернет-інструментів, зростає з кожним роком, і пов'язано це, насамперед, зі зростанням можливостей здійснювати різні фінансові, соціальні та інші види взаємодії в онлайн-просторі. Однак існує прямий взаємозв'язок між кількістю кіберзлочинів і рівнем науково-технічного розвитку тієї чи іншої країни. Згідно з Глобальним індексом інновацій, одними з найбільш інноваційно розвинених держав є Сполучені Штати Америки, Велика Британія, Японія, інтенсивність розвитку наукового прогресу яких у кілька разів перевищує аналогічний процес у менш розвинених державах, наприклад, у регіоні Центральної Азії. Роль і місце державних органів щодо запобігання інтернет-злочинам вкрай складно переоцінити, адже саме центральне та місцеве управління має провідні позиції в питаннях розроблення превентивних заходів із профілактики та мінімізації такого явища як віктимізація суспільства в інтернет-просторі. Розрізнення та розуміння видів і напрямів злочинів в онлайн-середовищі необхідне для створення ефективного механізму боротьби з такими злочинами та розробки дієвих інструментів для прищеплення здорового способу життя людини з метою запобігання розвитку в ній віктимних рис. Результати роботи можуть використовуватися як практична база для подальших досліджень за темою – розробка державних стратегій боротьби з кіберзлочинами

Ключові слова: колегіальне та одноосібне управління; права людини; науково-технічний потенціал; колегіальні та одноосібні представники публічної влади; хакерські атаки; Глобальний індекс інновацій; протидія інтернет-злочинності