Public Policy and Accounting
ISSN 2707-9325

UDC 321:004.056:007

Experience in Shaping the Legal Framework of State Policy on Combating Cybercrime in Post-Soviet Countries

Grytsyshen Dymytrii[1], Sokha Stanislav[2], Korzun Svitlana[3]

[1] Doctor of Science in Public Administration, Doctor of Economic Sciences, Professor
Zhytomyr State Polytechnic University

[2] PhD in Law, Doctoral Student
Zhytomyr State Polytechnic University

[3] Postgraduate student
Zhytomyr State Polytechnic University

Abstract

The article presents a comprehensive analysis of the experience of post-Soviet countries in shaping the legal framework of state policy on combating cybercrime. The Criminal Codes of the Republic of Uzbekistan, the Republic of Tajikistan, and Georgia are examined, with an assessment of the characteristics of these countries' national criminal law systems in terms of establishing liability for criminal offences in the field of cybersecurity. Key attention is given to such aspects as the transnational nature of cybercrime, effective investigation of crimes committed in the global network, cooperation between law enforcement agencies of different countries, and developing national legislation on cybercrime in Ukraine. The article explores the specific features of the criminal law of the Republic of Uzbekistan, the Republic of Tajikistan, and Georgia, identifying fundamental directions for transforming Ukraine's criminal legislation in the context of modern challenges and threats in cybercrime. The study of the legal framework for state policy on combating cybercrime in Uzbekistan, Tajikistan, and Georgia made it possible to determine the directions for transforming Ukraine's criminal legislation to expand the types of cybercrimes and establish criminal liability for their commission.

Keywords: state policy; combating cybercrime; cyberspace; criminal liability.

1. Introduction

The most important component of state policy on combating cybercrime is developing the legal framework for its implementation. In particular, the system of legal regulation in combating cybercrime must define criminal liability for such unlawful acts. Cybercrime is a relatively new object within the criminal law system and state policy for Ukraine and the world. "With the introduction of modern information technologies, the development of scientific and technological progress has led to the emergence of new types of crimes, including unlawful interference with the operation of electronic computing machines, computer networks and systems, theft, misappropriation, and manipulation of computer information. Therefore, this is collectively called a dangerous antisocial phenomenon known as 'cybercrime'" [5]. There are many conflicts regarding these types of criminal offences both in international criminal law and in various countries' criminal laws. When developing the legal mechanism of state policy to combat cybercrime, it is necessary to study international experience, which can be achieved by examining the criminal legislation of countries around the world.

Corresponding author:

[1] ORCID: https://orcid.org/0000-0002-1559-2403
[2] ORCID: https://orcid.org/0009-0004-2606-1263
[3] ORCID: https://orcid.org/0000-0002-8360-6766

doi: https://doi.org/10.26642/ppa-2024-2(10)-33-42

2. Analysis of recent research

The criminal law in foreign countries in general, and in the field of combating cybercrime in particular, has been explored in the dissertations of domestic scholars in the following scientific fields: public administration (D.O. Hrytsyshen, V.V. Yevdokymov, K.V. Malyshev, V.V. Nonik, I.V. Suprunova), legal sciences (T.V. Baranovska, S.O. Perkhun, M.M. Zabarnyi, O.I. Myrhorodskyi, E.V. Maliutin, M.O. Dumchykov, B.B. Teplytskyi, M.Yu. Yatsyshyn, O.M. Bodunova, V.V. Sysoliatin, T.A. Bilobrov) and economics (A.P. Dykyi, O.S. Kushneriov).

3. Results and discussion

"In recent decades, the world has undergone radical changes. Modern society can no longer imagine life without the internet, computers, smartphones, and other technological perks. Alongside the real world, the metaverse is developing, which may transform many aspects of our everyday lives. This is a consequence of the digital revolution, which is taking place thanks to the advancement of information and telecommunication technologies. Progress leaves no one indifferent, which has led to the emergence of a phenomenon such as cybercrime. Around the world, cybercrimes cause tens of billions of US dollars in damages yearly to governments and private companies. … Thus, cybercrime affects various areas of people's lives, and anyone can become its victim. The global community has declared the fight against cybercrime one of the priority areas of activity for their governments and law enforcement agencies, as the level of danger from illegal actions in cyberspace is extremely high" [2].

"One of the main characteristics of high-tech crime is its transnational nature, which means it is connected to multiple legal systems. Therefore, effective counteraction to cybercrime is impossible if investigating crimes, extradition of offenders, and prosecuting in court is complicated or entirely impossible due to significant differences in national criminal laws and relevant regional agreements. In fact, such inconsistency allows criminals to avoid liability, leaving their actions unpunished. Consequently, existing legislative acts based on the principle of nulla poena sine lege must include an exhaustive list of unlawful acts committed using ICT, making the creation of appropriate universal standards an objective necessity. One of the ways to address this issue is the study of criminal legislation in combating cybercrime in various countries around the world."

"Since no country can act solely at the national level to protect itself, a comprehensive fight against cybercrime requires:

– harmonizing criminal legislation on cybercrime at the international level;

– developing and implementing procedural standards at the international level into national legislation, to effectively investigate crimes in the global information network, obtain, examining, and presenting electronic evidence, taking into account the cross-border nature of this issue;

– establishing cooperation at the operational level between law enforcement agencies in the investigation of cybercrimes;

– mechanisms for resolving jurisdictional issues in cyberspace" [5].

The above should serve as the basis for developing and implementing state policy to combat cybercrime in Ukraine to ensure the state's information security. "The issue of cybercrime is extremely important at the state level. Critical infrastructure objects like energy facilities, transportation, and the banking sector often come under cyberattack. The cost of protection is usually ten times higher than the cost of the attack itself. Therefore, cybersecurity is a priority area in the policy of many countries" [1]. "Since most cybercrimes are committed for personal gain, the state's task is to create conditions where specialists will work for civil society rather than against it. At the same time, it is important to understand that for every computer 'genius', there is someone even more intelligent, and therefore, it is possible to uncover a cybercriminal all that is needed is a more qualified specialist. Ukraine needs further development of cybersecurity because only with an adequate level of it will the proper functioning of systems and networks – which are increasingly integrated into the daily life of our society become possible" [2]. Accordingly, it is proposed to identify the key features of national criminal law systems around the world that may provide both positive and negative experiences. It is worth noting that, in the context of European integration processes and the need to overcome the consequences of the Russian-Ukrainian war and counteract the information war, Ukraine must define its own model of legal counteraction to cybercrime. Studying foreign experience will make it possible to establish priority directions for transforming and improving the Criminal Code of Ukraine, both in terms of expanding criminal liability for certain types of acts and broadening aggravating circumstances.

"It is considered that the source of law is the external form of objectifying a legal norm. Only a norm that has been objectified (in a certain form) becomes a legally binding norm, the implementation of which is ensured by the appropriate means of state influence. This also applies to the norms of criminal law. The main sources of criminal law in most foreign countries are criminal codes (sometimes called criminal laws or certain sections within a body of laws). In most developed foreign countries, the source of criminal law is not limited to criminal codes. Such sources may also include constitutions, other laws and subordinate normative acts, judicial precedents (the latter is characteristic of the common law family), international treaties, and opinions of legal authorities, which is typical for English law; they may also include decisions of the European Court of Human Rights" [6].

To assess the characteristics of national criminal law systems around the world regarding the establishment of liability for criminal offenses in the field of cybersecurity, we will examine the Criminal Codes of a group of countries:

- countries that were part of the Soviet Union and share a common political past with Ukraine, and consequently, their legal systems are similar and have many common features. The Criminal Codes of the Republic of Uzbekistan, the Republic of Tajikistan, and Georgia will be studied in this context. It is worth noting that among the mentioned countries, Georgia intends to join the European community;

- which are members of the European Union, will serve as the basis for determining the priorities for developing a roadmap for the European integration of the national criminal law system. In particular, legislative acts of Central and Eastern European countries that were part of the socialist bloc and the Soviet Union, and that have successfully undergone the process of European integration and have been members of the European Union for a considerable time, will be studied. Specifically, the legal regulation of combating cybercrime (Criminal Codes) in countries such as the Republic of Bulgaria, the Czech Republic, the Republic of Lithuania, and the Republic of Poland will be examined.

Let's examine the Criminal Codes of the specified countries in the following format: firstly, a general overview of the primary document that governs criminal law as a whole and specifically in the context of combating cybercrime; secondly, identification and characterization of criminal offenses that are classified as cybercrimes and are subject to criminal liability in the country under study; thirdly, the definition of penalties and aggravating circumstances for cybercrimes.

Let's consider the substantive and formal characteristics of the criminal legislation of foreign countries, particularly those that were part of the Soviet Union, in relation to combating cybercrime.

The Republic of Uzbekistan. In the Republic of Uzbekistan, the primary document regulating the state's criminal policy is the Criminal Code of the Republic of Uzbekistan [4], [8], adopted by the Supreme Council of the Republic of Uzbekistan in 1994. Numerous amendments and additions have been made since its adoption, including significant changes in 2019 specifically related to combating cybercrime. According to the Criminal Code of the Republic of Uzbekistan, issues concerning liability for cybercrimes are regulated by Chapter XX.1 – Crimes in the Field of Information Technology. Currently, this chapter defines the following types of cybercrimes:

– *violation of informatization rules* – violation of the rules of informatization, i.e., the creation, implementation, and operation of information systems, databases, and data banks; systems for processing and transmitting information; unauthorized access to information systems without taking established protective measures, which caused significant harm or substantial damage to the rights or legally protected interests of citizens, or to state or public interests (Article 278.1);

- *illegal (unauthorized) access to computer information* refers to unauthorized access to computer information, i.e., information in information-computing systems, networks, and their components, if this action resulted in the destruction, blocking, modification, copying, or interception of information, or the disruption of the operation of electronic computing machines, electronic computing systems, or their networks (Article 278.2);

- *manufacturing for the purpose of distribution or distributing and disseminating special tools for obtaining illegal (unauthorized) access to a computer system* (Article 278.3);

- *modification of computer information* is a modification of computer information, namely, the unlawful alteration, damage, or erasure of information stored in a computer system, as well as the introduction of knowingly false information into it, which has caused significant harm or substantial damage to the rights or legally protected interests of citizens, or to state or public interests (Article 278.4);

- *computer sabotage* is the intentional disabling of someone else's or official computer equipment, as well as the destruction of a computer system (computer sabotage) (Article 278.5);

- *creation, use, or distribution of malicious programs* are the creation of computer programs or modifications to existing programs with the purpose of unauthorized destruction, blocking, modification, copying, or interception of information stored or transmitted within a computer system, as well as the development of specific virus programs, their intentional use, or distribution (Article 278.6);

- *illegal (unauthorized) access to the telecommunications network* is an illegal (unauthorized) access to the telecommunications network for the purpose of its use and routing international traffic bypassing established protection systems, as well as storing and creating conditions for the operation of specialized software or hardware tools intended for this purpose (Article 278.7);

- *violation of legislation in the field of cryptocurrency circulation* is an illegal acquisition, sale, or exchange of cryptocurrency assets, conducting activities as service providers in the field of cryptocurrency circulation without obtaining a license in the prescribed manner, or performing transactions with anonymous cryptocurrency assets by service providers in the field of cryptocurrency circulation, committed after the application of administrative penalties for similar actions (Article 278.8);

- *illegal conduct of mining activities* is defined as engaging in the mining of anonymous crypto-assets or conducting mining in violation of established procedures, committed after applying administrative penalties for similar actions (Article 278.9).

It is worth noting that Articles 278.8 and 278.9, which define liability for violations of legislation in the field of crypto-asset circulation and illegal mining activities, were adopted in 2024. This is logical, given the growing relevance and financial viability of cryptocurrencies. The studied regulatory document also establishes liability for specific cybercrimes, as presented in Table 1.

Analyzing the approaches of Uzbek criminal legislation to determining the degree of punishment for cybercrimes, it is worth emphasizing that the highest penalty defined by the Criminal Code of the Republic of Uzbekistan is a restriction of freedom for a term of three to five years for the following crimes:

-violation of legislation in the field of crypto-asset circulation if the illegal acquisition, sale, or exchange of crypto-assets is carried out using an official position, by an organized group, or in its interests. Under the same article, if no aggravating circumstances are identified, the penalty includes a fine of up to one hundred base calculation units, correctional labor for a term of two to three years, restriction of liberty for up to one year, or imprisonment for up to one year. The fine may be increased to between three hundred and four hundred base calculation units, or restriction of liberty for up to three years may be imposed if the following aggravating circumstances are present: the crime was committed by a group of persons by prior conspiracy, committed repeatedly or by a dangerous recidivist, or involved especially large amounts;

- illegal mining activities, if the mining of anonymous crypto-assets or mining conducted in violation of the established procedure is carried out after the imposition of an administrative penalty for the same actions, and is aggravated by such circumstances as the use of official position or being committed by an organized group or in its interests. Under the same article, without aggravating circumstances, the penalty provides for a fine of up to one hundred basic calculation units, or correctional labor for a term of two to three years, or restriction of liberty for up to one year, or imprisonment for up to one year. If the aggravating circumstances include prior conspiracy by a group of persons, repeated offense, or commission by a dangerous recidivist, or if committed on a particularly large scale, the punishment will be as follows: a fine ranging from three hundred to four hundred basic calculation units, or restriction of liberty for up to three years, or imprisonment for up to three years.

Table 1
Criminal Liability for Cybercrimes in the Republic of Uzbekistan

Cybercrime	Punishment	Aggravating Circumstances of Committing a Cybercrime (the Same Act Committed)				
		A[4]	B[5]	C[6]	D[7]	E[8]
1	*2*	*3*	*4*	*5*	*6*	*7*
Violation of Informatization Rules	A fine of up to fifty non-taxable minimum incomes of citizens or correctional labor for up to one year	-	-	-	-	+
		A fine of up to fifty non-taxable minimums				
Illegal (unauthorized) access to computer information	A fine of up to one hundred tax-free minimum incomes of citizens, or deprivation of a certain right for up to three years, or corrective labor for up to one year	+	+	+	+	-
		A fine from one hundred to three hundred non-taxable minimum incomes of citizens, or corrective labor from one year to two years, or restriction of freedom from one year to three years, or imprisonment for up to three years				
Manufacture for the purpose of sale, or the sale and distribution of special devices for obtaining illegal (unauthorized) access to a computer system	A fine of up to two hundred tax-free minimum incomes of citizens or corrective labor for up to one year	+	+	+	+	-
		A fine from two hundred to three hundred non-taxable minimum incomes of citizens or corrective labor from one year to three years				
Modification of computer information	A fine of up to one hundred non-taxable minimum income levels of citizens, or corrective labor for up to one year, or restriction of liberty for up to two years, or imprisonment for up to two years	+	+	-	-	+
		Correctional labor from one to two years, or restriction of liberty from two to three years, or imprisonment from two to three years				
Computer sabotage	A fine from three hundred to four hundred non-taxable minimum incomes of citizens, with the deprivation of a certain right for up to three years, or restriction of freedom for up to two years, or imprisonment for up to two years	+	+	-	-	-
		Corrective labor from two to three years, or restriction of liberty from two to three years, or imprisonment from two to three years				
Creation, use, or distribution of malicious software	A fine ranging from one hundred to three hundred non-taxable minimum incomes of citizens, or restriction of liberty for up to two years, or imprisonment for up to two years	+	+	-	+	+
		Imprisonment for a term of two to three years or deprivation of liberty for a term of two to three years				

[4] A – The same act committed by a group of persons by prior conspiracy
[5] B – The same act committed repeatedly or by a dangerous recidivist
[6] C – The same act committed with the use of official position
[7] D – The same act committed by an organized group or in its interests
[8] E – The same act committed with the infliction of especially large damage

End of the of table 1

1	*2*	*3*	*4*	*5*	*6*	*7*
Illegal (Unauthorized) Access to Telecommunications Network	A fine ranging from one hundred to three hundred basic calculated units, or imprisonment for a term of one to three years, or imprisonment for up to three years	+	+	+	+	-
		A fine from three hundred to six hundred basic calculation units, or restriction of liberty for three to five years, or imprisonment for three to five years				
Violation of Legislation in the Field of Crypto-Asset Circulation	A fine of up to one hundred basic calculation units, or corrective labor from two to three years, or restriction of freedom for up to one year, or imprisonment for up to one year	+	+	-	-	+
		A fine of three hundred to four hundred basic calculated units, or restriction of freedom for up to three years, or imprisonment for up to three years				
		-	-	+	+	-
		Imprisonment for a period of three to five years				
Illegal operation of mining activities	A fine of up to one hundred basic calculation units, or corrective labor from two to three years, or restriction of liberty for up to one year, or imprisonment for up to one year	+	+	-	-	+
		A fine of three hundred to four hundred times the minimum calculation amount, or restriction of liberty for up to three years, or imprisonment for up to three years				
		-	-	+	+	-
		Imprisonment for a period of three to five years				

Republic of Tajikistan. The Criminal Code of the Republic of Tajikistan [3] was adopted in 1998, and many amendments have been made over more than 25 years. The Criminal Code consists of the General Part and the Special Part. The Special Part provides for criminal liability for the following crimes:

– crimes against the person (against life and health, against personal freedom, honor and dignity, against sexual freedom or sexual inviolability, against constitutional rights and freedoms of individuals and citizens, against the family and minors);

– crimes against public safety and public health (against public safety, against public health, against traffic safety and the operation of transport);

– crimes related to environmental safety and the natural environment;

– crimes related to public order and morality;

– crimes in the field of economics (crimes against property, crimes in the field of economic activity);

– crimes against information security;

- crimes against state power (against the foundations of the constitutional order and state security, against state power, the interests of civil service, against the order of governance, against justice);

- crimes against military service;

- crimes against peace and the security of humanity.

The issue of combating cybercrime through the establishment of criminal liability and punishment measures is addressed in Chapter 28 – Crimes against Information Security, which defines the following criminal offenses:

- unauthorized access to computer information: unauthorized access to information stored in a computer system, network, or on machine carriers, accompanied by a breach of the protection system (Article 298);

- modification of computer information: altering information stored in a computer system, network, or on machine carriers, as well as introducing knowingly false information that caused significant damage or created a threat of such damage (Article 299);

-computer sabotage: destruction, blocking, or rendering computer information or programs unusable, disabling computer equipment, and damaging a computer system, network, or machine carrier (Article 300).

– illegal seizure of computer information: a) illegal copying or other unlawful acquisition of information stored in a computer system, network, or on machine carriers, as well as interception of information transmitted using computer communication; b) coercion to transfer information stored in a computer system, network, or on machine carriers, under the threat of disclosing disgraceful information about a person or their relatives, publishing information about circumstances the victim wishes to keep confidential, as well as under the threat of applying violence to the person or their relatives, or under the threat of destroying or damaging the property of the person, their relatives, and other individuals under whose management or protection the information is kept (Article 301);

– manufacturing and distribution of special tools for unauthorized access to a computer system or network: manufacturing for the purpose of sale, as well as the sale of special software or hardware tools designed to obtain unauthorized access to a protected computer system or network (Article 302);

– development, use, and distribution of malicious software – development of computer programs or modification of existing programs with the intent of unauthorized destruction, blocking, modification, or copying of information stored in a computer system, network, or on machine media, as well as the development of special viral programs, deliberate use of them, or distribution of carriers with such programs (Article 303);

– violation of the rules for operating a computer system or network – violation of the rules for operating a computer system or network by a person who has access to this system or network, if this has caused, through negligence, the destruction, blocking, modification of computer information, disruption of computer equipment operation, or caused other significant damage (Article 304).

This section defines the measure of punishment and the establishment of aggravating circumstances, which are systematized and presented in Table 2.

The aggravating circumstances under the Criminal Code of the Republic of Tajikistan are as follows:

- if they cause, through negligence, the alteration, destruction, or blocking of information, as well as the disabling of computer equipment or significant damage in relation to crimes such as Unauthorized Access to Computer Information;

- if they cause, through negligence, severe consequences related to the following crimes: unauthorized access to computer information; modification of computer information; computer sabotage; development, use, and distribution of malicious software; violation of the rules of operation of a computer system or network;

Table 2
Criminal Liability for Cybercrimes in the Republic of Tajikistan

Article	Punishment	Aggravating Circumstances of Committing a Cybercrime (the Same Act Committed)									
		A[9]	**B**[10]	**C**[11]	**D**[12]	**E**[13]	**F**[14]	**G**[15]	**H**[16]	**I**[17]	**J**[18]
Unauthorized access to computer information	A fine ranging from two hundred to four hundred calculation units or imprisonment for up to two years	+	-	-	-	-	-	-	-	-	-
		The fine ranges from three hundred to five hundred units for calculations, or corrective labor for a period of up to two years, or imprisonment for a period of up to three years									
		-	+	-	-	-	-	-	-	-	-
		The penalty is from 400 to 700 units for calculations or imprisonment for a term of up to four years									
Modification of computer information	The fine is from three hundred to five hundred calculation indicators, or corrective labor for up to two years, or imprisonment for the same period	-	+	+	-	-	-	-	-	-	-
		The penalty is from five hundred to one thousand index points for calculations or imprisonment for up to three years									
Computer sabotage	The fine is from two hundred to five hundred units of calculation, or imprisonment for up to two years, or arrest for up to four months	-	+	+	-	-	-	-	-	-	-
		The fine is from five hundred to one thousand calculation indicators or imprisonment for up to three years									
Unlawful seizure of computer information	a) A fine from two hundred to five hundred index points for calculations or imprisonment for up to two years b) Restriction of freedom for up to five years or imprisonment for a period of two to four years	-	-	-	+	+	+	+	-	-	-
		Imprisonment for a term of five to seven years									
		-	-	-	-	-	-	-	+	+	+
		Imprisonment for a term of seven to ten years.									
The manufacture and sale of special means for gaining unauthorized access to a computer system or network	A fine ranging from two hundred to five hundred units for calculations, or imprisonment for up to two years, or arrest for a period of two to six months	Aggravating circumstances are not defined									
Development, use, and distribution of malicious software	The fine ranges from three hundred to five hundred indicators for calculations or imprisonment for up to two years	-	+	-	-	-	-	-	-	-	-
		The fine ranges from five hundred to one thousand index points for calculations or imprisonment for up to three years									
Violation of computer system or network operation rules	The fine of up to three hundred index points for calculations, or imprisonment for up to two years	-	-	-	-	-	-	+	-	-	-
		The fine ranges from three hundred to five hundred units of account, or corrective labor for up to two years, or imprisonment for the same period									
		-	+	-	-	-	-	-	-	-	-
		The fine ranges from 500 to 1000 indicators for calculations or imprisonment for up to three years									

[9] A – if they caused by negligence a change, destruction, or blocking of information, as well as the failure of computer equipment or significant damage
[10] B – caused by negligence serious consequences
[11] C – combined with unauthorized access to a computer system or network
[12] D – related to the use of violence against a person or their close relatives
[13] E – committed by a group of individuals by prior agreement
[14] F – caused significant harm to the victim
[15] G – committed with the intention of obtaining especially valuable information
[16] H – committed repeatedly
[17] I – committed by an organized group
[18] J – caused by negligence the death of a person or other serious consequences

– combined with unauthorized access to a computer system or network. This aggravating factor is attributed to the following types of cybercrimes: modification of computer information; computer sabotage;

– related to the use of violence against a person or their relatives in relation to the crime of illegal seizure of computer information;

– committed by a group of persons with prior conspiracy concerning the illegal seizure of computer information;

– caused significant harm to the victim, also defined within the framework of the article "Illegal seizure of computer information";

– committed to obtain especially valuable information, foreseen for such crimes as illegal seizure of computer information; violation of the rules for the operation of computer systems or networks;

– committed repeatedly, applies only to the illegal seizure of computer information;

- committed by an organized group also applies only to the illegal acquisition of computer information;

- causing the death of a person or other severe consequences by negligence is considered an aggravating circumstance for the crime of illegal acquisition of computer information.

A feature of the specified regulatory document is the definition that cybercrimes can lead to the death of a person. Accordingly, under such aggravating circumstances, the punishment is seven to ten years imprisonment.

Georgia. The Criminal Code of Georgia was adopted in 1999, and it has undergone many amendments over such a long period. The Special Part of the Criminal Code of Georgia provides for responsibility for the following types of crimes:

– crimes against the person (against life, against health, creating threats to life and health, against sexual freedom and inviolability, against human rights and freedoms, against family and minors);

– economic crimes (against property, against entrepreneurial or other economic activities, in the areas of the monetary and credit system, financial system, against the interests of service in entrepreneurial or other organizations);

– crimes against environmental protection and natural resource usage (against environmental protection);

– crimes against humanity (against peace, human security, and international humanitarian law);

- crimes against public safety and public order (against public safety and public order, violations of safety rules during work, against the health of the population and public morality, against cultural heritage, international crimes against cultural heritage, crimes related to narcotics, transport crimes, cybercrimes);

- crimes against the state (against the foundations of the constitutional order and the security of Georgia, violations of the legal regime of occupied territories, terrorism, official crimes, against the order of governance); - crimes against judicial authority (against the activities of judicial bodies, against the procedural order of evidence gathering, against timely prevention and detection of crimes, against the execution of judicial acts);

- crimes against military service (against the order of subordination and adherence to military honor, against the order of storage or use of military property).

The issue of cybercrime is addressed in Chapter XXXVV, which came into effect in 2010. This section provides for criminal liability for the following types of crimes:

– unauthorized access to a computer system (Article 284);

– illegal use of computer data or (1) computer systems – unauthorized creation, storage, sale, distribution of computer programs or (and) other devices, as well as passwords, access codes necessary for penetrating a computer system, or other similar data or other means of accessing them with the intent to commit a crime (Article 285);

– attacks on computer data or (and) computer systems – unauthorized damage, destruction, substitution, or concealment of computer data (Article 286).

- intrusion into computer data or computer systems for financial gain – unauthorized access to a computer system, unauthorized modification, destruction, substitution, or concealment of computer data to acquire property rights or obtain any financial gain for oneself or another person, or any unauthorized interference with the functioning of a computer system that causes financial harm to another person (Article 286.1);

- creation of counterfeit official computer data – obtaining counterfeit official computer data by unauthorized modification, destruction, substitution, or concealment of computer data with the intention of selling or using them as genuine/valid data, their sale or use (Article 286.2).

Criminal liability and aggravating circumstances according to the Criminal Code of Georgia are presented in Table 3. Thus, the mentioned code provides for a combination of aggravating circumstances:

Table 3
Criminal liability for cybercrimes in Georgia

Article	Punishment	Aggravating Circumstances of Committing a Cybercrime (the Same Act Committed)							
		A[19]	B[20]	C[21]	D[22]	F[23]	G[24]	H[25]	I[26]
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
Unauthorized access to a computer system	A fine or correctional labor for up to two years, or imprisonment for the same term	+	+	+	+	-	-	-	-
		Fine or corrective labor for a term of up to two years, or imprisonment for a term of two to five years							
		-	-	-	-	+	-	-	-
		Imprisonment for a term of three to six years							
Illegal use of computer data or (1) computer systems	A fine or corrective labor for a term of up to two years or (and) imprisonment for a term of up to three years	+	+	+	+	-	-	-	-
		A fine or corrective labor for a term of up to two years or (and) imprisonment for a term of three to six years							
		-	-	-	-	+	-	-	-
		Imprisonment for a term of four to seven years							
Intrusion into computer data or computer systems for financial gain	Community service for a term of one hundred seventy to two hundred hours, or correctional labor for a term of up to two years, or house arrest for a term of one to two years, or imprisonment for a term of two to four years	+	-	-	-	-	+	-	-
		Imprisonment for a term of five to seven years							
		-	-	+	+	-	-	+	+
		Imprisonment for a term of six to ten years							
		-	-	-	-	+	-	+	-
		Imprisonment for a term of seven to eleven years							
Creation of counterfeit official computer data	A fine or imprisonment for a term of up to three years	-	+	+	+	-	-	-	-
		Imprisonment for a term of three to six years							
Attacks on computer data or (and) computer systems	A fine or corrective labor for a term of up to two years or (and) imprisonment for the same term	+	+	+	+	-	-	-	-
		A fine or corrective labor for up to two years, or imprisonment for a term of three to five years							

[19] A – committed by a group of persons by prior agreement
[20] B – committed using official position
[21] C – committed repeatedly
[22] E -caused significant harm
[23] F – committed against a critical infrastructure subject
[24] G – caused significant financial losses
[25] H – committed by a person who has been convicted two or more times for unlawful appropriation or extortion of another's property/another's property rights, or for committing a crime
[26] I – – committed by an organized group

– committed by a group of persons with prior conspiracy;
– committed using official authority;
– committed repeatedly;
– caused significant harm;
– committed against a critical infrastructure entity;
– caused significant financial losses;
– committed by a person previously convicted two or more times for unlawful appropriation or extortion of another's property / rights to property or for committing a crime;
– committed by an organized group.

The specified aggravating circumstances in almost all cybercrimes define the punishment as imprisonment. The longest term of imprisonment ranging from seven to eleven years is stipulated for offenses involving unauthorized access to computer data or systems with the intent to obtain financial gain, provided that such a crime is committed against a critical infrastructure entity or by a person previously convicted two or more times for unlawful appropriation or extortion of another's property/rights or for committing a similar offense.

4. Conclusions

The study of the experience of the aforementioned countries in establishing criminal liability for cybercrimes allows for the identification of directions for transforming Ukraine's criminal legislation. Considering the full-scale war, modern financial instruments, and geopolitical transformations, it is important to take the following experience into account when improving criminal legislation:

- firstly, criminal liability in the illegal handling of crypto-assets should be established. Domestic criminal legislation does not provide liability for criminal offenses related to crypto-assets. Accordingly, it is necessary in Ukraine to regulate this issue from the perspective of commercial, financial, monetary, and tax legislation and criminal liability for violations involving crypto-assets;
- secondly, to provide for criminal liability or define as an aggravating circumstance cybercrimes related to critical infrastructure. This will enable the implementation of effective tools to counter cyberattacks on critical infrastructure and outline directions for ensuring the state's cybersecurity;
- thirdly, the expansion of aggravating circumstances through establishing such factors as: significant financial losses for the state, business entities, or individuals; the commission of a cybercrime by an official or through their mediation.

Thus, studying the experiences of the Republic of Uzbekistan, the Republic of Tajikistan, and Georgia has made it possible to identify directions for transforming Ukraine's criminal legislation to expand the types of cybercrimes and criminal liability for their commission.

References:

1. Holub, A. (2016), «Cybercrime in All Its Forms: Types, Consequences, and Methods of Combating It», [Online], available at: https://www.gurt.org.ua/articles/34602/
2. Kryvenko, K. (2022), «Cybercrime: Current Judicial Practice», [Online], available at: https://biz.ligazakon.net/analitycs/209283_kberzlochinnst-aktualna-sudova-praktika
3. Stanich, V.S. (2019), *Criminal Code of the Republic of Tajikistan*, Translated by Menchen, K.V., in Menchinsky, V.L. (ed.), OVK, Kyiv, 288 p.
4. Stanich, V.S. (2019), *Criminal Code of the Republic of Uzbekistan*, Translated by Ivanov, O.V., in Menchinsky, V.L. (ed.), OVK, Kyiv, 194 p.
5. Toshchakova, A.S. (2021), «Problems of combating cybercrime: international experience», *International law in the period of turbulence in international relations: a collection of materials from the All-Ukrainian Scientific Student Internet conference*, Helvetica Publishing House, Odesa, pp. 64–66, [Online], available at: https://dspace.onua.edu.ua/server/api/core/bitstreams/9bde68f6-dd4d-44c9-889e-41384216b4b0/content
6. Yatsenko, S.S. (2013), *Key Issues of the General Part of Criminal Law of Foreign States*, educational manual, Dakop, Kyiv, 168 p.
7. Yatsyshyn, M.Yu. (2018), «Criminalization of Cybercrimes in International Law: A Comparative Analysis», *Forum of Law*, No. 53 (5), pp. 92–99, [Online], available at: http://forumprava.pp.ua/files/092-099-2018-5-FP-Yatsyshyn_12.pdf
8. The Criminal Code of the Republic of Uzbekistan, [Online], available at: https://www.lex.uz/docs/111453
9. Legislative Herald of Georgia, [Online], available at: https://matsne.gov.ge/ka/document/view/16426?publication=264