International Journal of Safety and Security Engineering
Vol. 12, No. 4, August, 2022, pp. 481-490
Journal homepage: http://iieta.org/journals/ijsse

Cybercrime as a Threat to the National Security of the Baltic States and Ukraine: The Comparative Analysis

Mykhailo Dumchykov, Maryna Utkina, Olha Bondarenko*

Academic and Research Institute of Law, Sumy State University, Sumy 40007, Ukraine

Corresponding Author Email: o.bondarenko@yur.sumdu.edu.ua

https://doi.org/10.18280/ijsse.120409

Received: 21 January 2022
Accepted: 29 June 2022

Keywords:
international cooperation, cybercrime, cybercrime prevention, cybercrime types

ABSTRACT

The article is devoted to comparative legal research of cybercrime as a threat to the national security of the Baltic States and Ukraine. The purpose of the scientific article is to study the systems of criminal legislation in the part of cybercrime in the Baltic States and Ukraine, to determine the public danger of cybercrime, as well as to study ways of countering this criminal category. The object of research is cybercrime as a criminal and legal category. The subject of the study is the peculiarities of combating cybercrimes in the Baltic States and Ukraine, and carrying out a comparative analysis of their criminal legislation. The authors analyze the essence of the concept of cybercrime and identify the main types of cybercrime that are committed most often. Thus, in this article, "cybercrime" means any crime committed with the help of information technologies or in the information space. Special attention is focused on cybercrime in the Baltic States, in particular Latvia, Lithuania, and Estonia. The main types of cybercrimes, the responsibility for the commission of which is provided for by Chapter XVII of the Criminal Code of Ukraine, are described. The Convention on Cybercrime was considered, and it was determined which norms should be implemented in the legislation of the Baltic countries and Ukraine. It was determined that the issue of countering cybercrime in the Baltic States. The main threats, prevention, and countermeasures against cybercrimes in the Baltic States and Ukraine and the main features of international and legal cooperation with cybercrimes within the framework of the European Union are outlined. It was concluded that in order to combat crimes committed with the use of modern information technologies in Ukraine, it is necessary to constantly increase the security of information systems, develop modern information technologies, improve legislation in the field of information crimes, develop competitive means of informatization, expand international cooperation in the field of safe use of information resources.

1. INTRODUCTION

We live in the age of an information-oriented society when computers and telecommunications systems are all-encompassing. But humanity, harnessing telecommunications and global computer networks to better them, did not foresee what opportunities for abuse create information technology. Today, the victims of criminals operating in cyberspace can be not only people but also entire states. Thus, the safety of thousands of users can appear depending on several criminals. The number of criminal offenses committed in cyberspace is growing in proportion to computer network users. According to the International Criminal Police Organization and European Police Office, the rate of criminal offense growth. The actively used term "cybercrime" needs a detailed interpretation. In the narrow sense, "computer criminal offense" is a set of criminal offenses, where the main object of illegal encroachment are legally protected public relations in the field of secure creation, storage, processing, and transmission of computer information, and the subject of the criminal offenses is computer information, means of protection of computer information, information and telecommunication networks, means of storage, processing, and transmission of computer information". In a broad sense, the definition of "computer criminal offenses" is given the following interpretation: "computer criminal offenses is a set of criminal offenses where the main direct object of illegal encroachment are public relations in the field of computer information and information technology, safe operation of means of creation, storage, processing, transmission, protection of computer information, but computer information, information and telecommunication networks; means of creating, storing, processing, transmitting computer information (computers, smartphones, iPhones, cash registers, ATMs, payment terminals and other computer devices) are not only in front of the objects of the criminal offenses but also used as a means and criminal offenses commitment. In the given article the authors made reviews on such issues: types of cybercrimes; status and issues of cybercrimes in the Baltic States; main threats and cybercrime prevention and the Baltic States and Ukraine; present day cybercrime trends in Ukraine; international legal cooperation peculiarities in the fight against cybercrime within the European Union.

2. THEORETICAL FRAMEWORK OR LITERATURE REVIEW

As you know, in the mid-70s last century, a technically economic wave, based on information and communication technologies, has begun in society. Several decades have passed, and today we can state that information and communication technologies have gained access almost to all spheres of human life, and the world of law is not an exception. In recent years, citizens' general and professional lexicon has included coined words: informatization, digital technologies, digitalization, digital reality, virtual reality, information and communication space, and information culture. Criminal offenses in the electronically stored information field are dangerous acts for society, committed with intent or recklessly, threatening computer information security, and can inflict harm to the benefits protected by law (individual rights, property relations, etc.).

The flashy growth of cyber threats in present-day society poses a highly urgent task for every state – the need to ensure information security. The annual world assessment of this criminal offense type raises fears due to the low level of citizens' protection in the modern information society; herewith, the range of problems is quite broad – from technical insecurity to the work support systems vulnerability, meant for cash transactions.

It should be noted that all cybercrimes are committed in cyberspace, where it directly acts as the place where the crime was committed. Fureshev defines the concept of cyberspace as a form of coexistence of a set of material and immaterial objects and processes aimed at generation, perception, storage, processing and exchange of information [1].

At the same time, analyzing scientific studies in the field of cybercrimes, it may be concluded that most indigenous articles and monographs on this topic pose it as a natural and imminent risk to the current order; the only way to deal with it is to limit and control cyber relations [2].

Even though the study of the given issue has been going on for decades, the concept of cybercrime is not fully formed, allowing a wide "deployment" of criminal groups. However, even illegal activity is one of the features of the society development stage. The origin, development, and spread of cybercrimes are part of modern human history, not a separate state. Danger to the public of this issue is considered worldwide, which is expressed in the relevant decisions of international organizations. First, it is a definition of the "cybercrime" concept. It is given in the recommendations of United Nations experts: "cybercrime" is any kind of criminal offense, which can occur through a computer system or network, within a computer system or network, or against a computer system or network [3]. Also, it should be noted that the European Commission defines cybercrime as "criminal acts committed using electronic communications networks and information systems or against such networks and systems" [4]. Jonathan Clough noted that the term "cybercrime" is used to define the criminal offenses committed or facilitated by the use of digital technologies and includes both already existing criminal offenses, for example, fraud or child pornography, and also an activity that is targeted at the technology itself, thus criminal offenses that are possible only because of the existence of the technology (for example, spamming or Distributed Denial of Service (DDoS) Attacks) [5].

It should be clarified that the specified term of an international legal definition of cybercrime is not limited. "Classic" types of criminal offenses committed through the use of cyberspace can also be included in the considered category. Accordingly, the definition of the concept "criminal offense committed in cyberspace" was defined. It should be understood as an unwarrantable interference with computers, computer programs, computer networks, unauthorized modification of computer data, and other unwarrantable socially dangerous actions committed with the help or using the computers, computer networks, and programs. In addition to the international legal definition of cybercrimes, there are also several scientific developments on this issue. For example, in his scientific study, Khusyainov [6] gives the following interpretation to the concept of "Internet criminal offense" or "cybercrime" as the full range of criminal actions in the field of information technology".

One major problem is that the concept of cybercrime is complex, and it encompasses a comprehensive range of different criminal offenses; some can be assessed through an economic perspective, while others are motivated by ideology, passion, and even revenge [7].

It should be noted that in modern legal literature under "cybercrimes" is understood as "criminal offenses in the computer information field," "information criminal offenses," "criminal offenses related to computer technical means," "criminal offenses in the information space" etc. According to Nomakov and Tropina, the concept of "cybercrime" is broader than "computer criminal offense" and fairly presents such a phenomenon as a criminal offense in the information space [8]. Significantly cyberspace is a space that is simulated and not limited to electronic devices. We believe that Karpova provides a complete definition reflecting aspect of this negative phenomenon, namely "cybercrime is an act of social deviance to inflict economic, political, moral, ideological, cultural and other types of harm, individual, organization or state through any technical means with access to the Internet [9].

Essentially the legal aspects are not reflected but have socio-economic problems of modern society. Batukhtin gives a broader definition of the concept of "cybercrimes" in his scientific study. "Cybercrime" should be understood as any criminal offense in the electronic sphere committed by or against computer means or virtual networks [10]. Thus, it is possible to define the terminology for this study. In this article, "cybercrime" is understood as any criminal offense committed with the help of information technology or in the information space. Herewith information technologies are understood by technical means (personal computers, laptops, smartphones), and the information and its carriers. And information space in the given article is understood as information and telecommunication networks (for example, the Internet), computer local networks.

Now the Criminal Code of the Baltic states (Estonia, Lithuania, Latvia) does not define the concept of "cybercrime." As well, the definition of "cybercrime" is absent in the Criminal Code of Ukraine. Still, in the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine, cybercrime is defined as a socially dangerous guilty act in cyberspace and with its use, the responsibility for which is punishable under the Law of Ukraine on criminal liability and which is recognized as a criminal offense by international treaties of Ukraine.

3. METHODOLOGY

The authors used the following general and special methods: descriptive method (revealing the essence of the concept of "cybercrime", outlined types of cybercrime, method of scientific analysis and generalization, as well as comparative (to study the features of international legal cooperation in combating cybercrime within the European Union). In addition, systemic and prognostic methods have been used to characterize existing measures to prevent and combat cybercrime in the Baltic States and Ukraine, as well as dialectical (to formulate the conclusions of the article). The paper combines general scientific and unique methods, which in complex implementation allowed to achieve positive research results. The authors used the analytical method to determine the main threats and cybercrime prevention; descriptive method to reveal some concepts, conduct an available description of the elements of the cybercrime's prevention. The authors used the comparative-legal method to compare the cooperation peculiarities in the fight against cybercrime in the Baltic States and Ukraine.

4. TYPES OF CYBERCRIMES

The first international regulatory and legal act defining the list of cybercrimes was the "Cybercrime Convention", which was adopted by the Council of Europe on November 23, 2001.

The authors note that the Convention does not define the concepts of "cybercrime" and "cyberspace", but only gives a list of cybercrimes, defines the measures that the state must implement at the national level, as well as certain methods of gathering and researching evidence [11]. It describes four types of computer criminal offenses, which are defined as illegal acts against the confidentiality, integrity, and admissibility of computer data and systems:

1) illegal access (Art. 2);
2) illegal wiretap (Art. 3);
3) interference with data (Art. 4);
4) interference with the system (Art. 5);
5) abuse of devices (Art. 6);
6) counterfeit related to computers (Art. 7);
7) computer-related fraud (Art. 8).

Four distinctions of cybercrimes from terrestrial criminal offense can be made: it is easy to learn how to commit a crime in cyberspace, relatively few resources are needed for the commission of a criminal offense compared to the damage it causes, cybercrime can be executed from any jurisdiction in any jurisdiction without physically being there, and often such criminal offenses are 'not illegal' as there is no clear 'signposting' of jurisdictions in cyberspace and also while an act is illegal in one jurisdiction, it might be not outlawed in another [12].

The following features characterize most criminal offenses committed on global computer networks:

1. increased stealth of the criminal offense;
2. cross-border nature of network criminal offenses, in which the perpetrator, the object of criminal inspiring and the victim may be in the territories of different states;
3. the possibility of committing a criminal offense in an automated mode in several places at the same time;
4. ignorance of victims that they were exposed to criminal influence;
5. remote nature of criminal actions in the absence of physical contact between the perpetrator and the victim;
6. inability to prevent and stop the criminal offense of this type by traditional means.

The specifics of the criminal offense scene are due to the need to use specialized tools, namely certain information technologies, which are already the main feature of cybercrimes.

Agreeably, cybercrimes can be classified into two main types: computer criminal offenses and criminal offenses committed in cyberspace. Such division is carried out at the criminal offenses' scene and the subject of endeavor. Most commonly, computer criminal offenses are aimed at obtaining illegal access to information (to take possession, change, or destroying) that is in the memory of a particular personal computer or improperly connected to a computer network for the same purposes. The subject of endeavor is information that the perpetrator of a criminal offense intends to destroy, change, block access to it, or unlawfully take possession of it by removing or copying. In turn, criminal violations committed in cyberspace generally completely copy the components of the "classic" variation of a criminal offense but occur using specific tools (for example, fraud in the field of Internet sales and purchases). The subject of such criminal endeavor can be almost anything: cash, information, weapons, narcotic drugs, etc.

In our opinion, taking into account social and economic dangerousness, the following types of cybercrimes should be highlighted:

Carding – the usage in transactions of payment card details received by the cracked file servers of online stores, payment and settlement systems, as well as from personal computers (either directly or through remote access programs, "Trojan horse", "bots"). It should be noted that carding can also be divided into two subspecies. Real carding is the process of obtaining a dump by the perpetrator of a criminal offense for its further application to the ingot using specific devices (for example, encoder). Material carding – the process of obtaining information about a bank card and the information about the cardholder for any financial transactions using the Internet. The material carding includes obtaining information about a bank card and obtaining documents confirming the identity of the cardholder (credit card holder) for further purchases over the Internet. A straw person is used in real carding, the so-called drop (a person who receives purchases made online). The ordered things come to the drop address. Most often, it is household appliances. Most often, this type of carding is carried out abroad.

Phishing (comes from fishing) is the pry of information from trusting citizens to access bank accounts. It is common in states where Internet banking services are popular. The essence of phishing lies in the fact that perpetrator of criminal offenses chooses the most popular sites and create their clone site, whose domain name differs from the original one or two characters. Such sites typically offer products or services. To order a consequence, the client must enter the details of their payment card. However, goods on such sites are not sold, and the primary goal of their administrators is to collect data from the maps of potential buyers for further acquisition of their funds. E-mail and other communications may be used to commit fraud. Quite often, fraudsters use information about the bank's customers received from unscrupulous employees of these same banks, allowing them to mislead the victim further. A person can also report to the lottery and ask for the card's details for sending money, etc. The study of phishing as

cybercrime in the field of Internet fraud involves the determination of the regulatory framework that regulates this issue [13]

So, at the international level, the United Nations solve the issue of counteraction to cybercrime through the introduction of the Global Cybersecurity Program (GCA), which includes the following areas: (1) legal measures; (2) technical and procedural measures; (3) organizational structures; (4) program of raising competence; (5) international cooperation [14].

Vishing (voice phishing) is a typical kind of network fraud. Vishing is similar to phishing. The difference between vishing from phishing is that the vishing uses the phone. The fraud scheme at the vishing is that the message contains a request to call a specific city number. Herewith, this reads a statement in which the potential victim is asked to disclose their confidential information. For example, enter the card number, passwords, PIN codes, access codes, or other personal information [15].

Online fraud can include fake online auctions, online stores, sites, and telecommunications facilities. The most widespread are various types of scam cryptocurrency exchangers. Also, it should be noted that the popular online fraud scam online stores, whose main activity is to sell popular products at a meager price, but the problem is that these products are not sent to the buyer.

Piracy is the illegal distribution of intellectual property on the Internet. Copyright in its main ideas was formed long before the formation of the Internet, which causes difficulties on the legality of actions taken as themselves understandable: reproduction, exchange, the publication of works, copying and pasting of text, images, and others. The legislation of most countries requires that these actions take place on the decision of the author. There was a need to balance the reality of online relationships and copyright legislation.

Malware – creation and distribution of viruses and malware. This type of cybercrime includes the following malware:

- Clipper – software that automatically changes the number of the electronic wallet of the person sending funds online to the electronic wallet of the software distributor's identity when infected.

- Styler is the software functionality that entirely consists of stealing passwords stored in the system and sending them to a person who uses viral software.

- Ransomware (virus) (contamination of words ransom and software) is considered a type of malware designed to extortion, block access to the computer system, or prevent reading the data recorded in it. It then requires the victim to ransom restore the original state.

Unlawful content we think should include:

- Cyber pornography - includes pornographic sites that allow visitors to place pornographic films, videos, and photos with minor citizens. In our opinion, this subspecies should be included dating websites which contain pornographic information about users and description of virtual sex with little citizens.

- Cyber dope-pushing - is a drug trade using the latest technology for message encryption transmitted by customers via email. In such messages, drug dealers indicate in coded form the place and method of exchanging goods for funds.

- Cyberterrorism is the commission of terrorist acts in cyberspace. This category of criminal offenses may include the simple dissemination over the Internet of information about terrorist attacks that can be carried out in the future at an expressly specified time.

5. CYBERCRIME IN THE BALTIC STATES: CURRENT STATUS AND CURRENT ISSUES

Security in current conditions becomes a category operated by scientists of the humanities and social disciplines, including social philosophy, political science, philosophical anthropology and sociology, social psychology, and international law. Security is of great importance in global politics and international relations, and its various aspects are regulated at the international legal level. The appliance of the basics of security theory will allow us to consider both civil and forceful approaches to cybersecurity and perceptions of potential threats and their sources. So, it should be investigated the cybersecurity policies of some Baltic states. Various doctrines review cybersecurity issues.

The national security paradigm reflects the state's traditional role in ensuring the country's borders and respect for the rule of law [16]. Cybersecurity is now recognized as fundamental to state military and economic security, and its necessity is justified by traditional national security arguments based on state protection.

Among all the countries of the former USSR, the experience of Estonia in the implementation of cyber security policy is the closest to the legislative regulation of Ukraine.

The state has developed and adopted strategic documents in the given area established appropriate institutional structures. Strategic planning ensures the cohesion of the entire cybersecurity architecture. In 2008, the Republic of Estonia was one of the first to adopt the National Cyber Security Strategy, inscribed in the framework of international law. Estonia began to create conditions that facilitate information and communication technologies and the creation of "smart solutions". Estonian Foreign Minister M. Kaljurand speaking in Brussels Europe in 2016at the conference on Internet governance in Europe EuroDIG (European Dialogue on Internet Governance), said that the development of cybersecurity should be part of people's daily lives, not a "luxury product".

Since 2011, coordinating Estonia's cybersecurity policy has generally shifted from the Ministry of Defense to the Ministry of Economic Affairs and Communications. Estonia's Cybersecurity Council, being an interagency body, supports interagency cooperation at the strategic level and oversees the implementation of the country's cybersecurity strategy goals.

The Ministry of Defense is a coordinating body for cyber defense in the field of national security. Since 2008, the Estonian Defense Forces have found a NATO Cyber Defense Centre of Excellence, an International Military Organization that focuses on empowering NATO and partner cyber defense capabilities. NATO has officially recognized cyberspace as an operational environment and thus equated existing threats to military threats.

In 2017, the NATO Cooperative Cyber Defense Centre of Excellence was established in Tallinn, the flagship of European cybersecurity. The Centre has received NATO accreditation, with 20 participants - 17 NATO members and three partner states. It employs and serves members, civilians, and representatives of the Government of the Republic of Estonia. The Center's work focuses on three main areas: research, training, and studying. The Center's main task is to train specialists from different countries who ensure security

in the national cyberspace. According to the Center M. Maigre director, "the most dangerous cyber threats are those that are supported at the state level." The center annually conducts the world's most effective cyber training, "Locked Shields," for cybersecurity experts. In 2017, NATO's Cyber Center exercise titled "Locked Shields 2017" took place in Tallinn, attended by about eight hundred professionals from 25 countries in information technology, international law, special services, science, and media. The Center's staff is developing a doctrine on cybersecurity, i.e., a single algorithm for action in case of cyber threats. It is planned that NATO will approve the new philosophy in 2019. All this indicates the intensification of work on the virtualization of security, including the military.

In the Republic of Latvia, the Cyber Security Strategy for the period 2014-2020 was adopted. The given Strategy considers threats related to the security of information and communication technologies in cyberspace and is given a forecast on cybersecurity risks for the future. According to the Latvian Information Technology Security Law, the essential safety requirements as to the state and municipal institutions, providers of public electronic communications are defined [17]. The two documents reflect a comprehensive approach to security protection in cyberspace and the national security of Latvia as a whole. Within this policy, the following areas of activity are defined: cybersecurity management, law enforcement in cyberspace and reducing cybercrime, education of society, and research work in this area, international cooperation.

There is a NATO cybersecurity Centre in Estonia and a NATO Energy Centre in Lithuania. The Ministry of Defense of the Republic coordinates Latvia's participation in the formation of international policy in cybersecurity following the general document - "Cyber Defense Pledge".

In the Republic of Lithuania, the regulatory regulation of cybersecurity has passed a long evolution from the establishment of cybersecurity institutions to the adoption of the law on cybersecurity. According to the Global Cyber Security Index compiled by the International Telecommunication Union, Lithuania ranks 57th. Overall, this index reflects the level of cybersecurity of states and the efforts made by a particular country to improve this indicator. Weaknesses in Lithuanian cybersecurity include the following [18]:

- low standards in organizations, insufficient level of social.
- incentives and interstate agreements.

Lithuanian authorities have repeatedly expressed a desire to assume the role of the leader in cybersecurity issues both in the European Union and in cooperation with the United States. In June 2018, the Sejm of Lithuania adopted amendments to the law on cybersecurity. Consequently, a review of national cybersecurity strategies in the Baltic states showed that their cybersecurity strategies are becoming comprehensive. These strategies cover economic, social, international legal, law enforcement, military aspects of cybersecurity. It should be mentioned that the Baltic states recognize the relationship between cybersecurity and national security and realize that cybersecurity issues, such as the destruction of the information and communication technology system or critical infrastructure, can harm national security and the effective functioning of the state economy.

Each of the considered Baltic states has its cybersecurity strategy and relevant laws to address cybersecurity concerns. Estonia, Lithuania, and to some extent, Latvia militarized cybersecurity issues. This trend raises cybersecurity to the level of national security and focuses on protecting public resources of information and communication technologies. In particular, Estonia and Lithuania tend to identify cybersecurity problems as threats to the normal functioning of the state and identify attacks by foreign states as the most dangerous sources of such threats. In these states, responsibility for neutralizing cyber threats is transferred to security agencies.

6. PRESENT-DAY CYBERCRIME TRENDS IN UKRAINE

We live in the age of an information-oriented society when computers and telecommunications systems are all-encompassing. But humanity, harnessing telecommunications and global computer networks to better them, did not foresee what opportunities for abuse create information technology. Today, the victims of criminals operating in cyberspace can be not only people but also entire states. Thus, the safety of thousands of users can appear depending on several criminals. The number of criminal offenses committed in cyberspace is growing in proportion to computer network users. According to the International Criminal Police Organization and European Police Office, the rate of criminal offense growth.

It should be noted that cybercrime is one of the global dangers for both the world and Ukraine. Cybercrime is a consequence of the information and communication technologies globalization and the emergence of international computer networks. Unlike other criminal offenses in Ukraine, cybercrime is currently the fastest-growing section due to the increase in the number of computer users connected to the global Internet, the constant increase in cybercriminals' professionalism, sustainable development, and improvement of information technology.

Any information and technical innovations greatly expand the scope of cybercrime and create conditions for increasing the effectiveness of hacking attacks. Cybercrime is therefore growing at a faster rate than all other types of criminal offense. Thus, according to the World Economic Criminal offense Survey Price Waterhouse Coopers (PWC) for 2019, against the background of a slight decrease in economic criminal offense in Ukraine, cybercrimes showed the highest rate for the entire period of publication of reviews.

According to statistic data of the Cyber Police Department of Ukraine for 2020, 11131 cybercrimes were registered, of which:

1) 1,139 in the field of illegal content;
2) 3,697 in the field of payment systems;
3) 3607 in the field of e-commerce;
4) in the field of cyber security.

At the same time, only 80% of the specified cybercrimes are traditional, and 20% are cybercrimes, which are provided for in Chapter 16 of the Special Part of the Criminal Code of Ukraine.

It is worth noting that because of the quarantine restrictions of COVID-19 and the consequences of Russia's armed aggression, the Cyber Police Department of Ukraine predicts a sharp increase in the level of cybercrime in 2023 [19].

To protect against hackers, cybersecurity costs are rising sharply in economically developed countries. Currently, in Ukraine, there is no responsibility for phishing and spam. At the same time, the components of the criminal offense "theft from a bank account", "theft from a credit card" was not even identified. And the maximum punishment provided by the

current legislation does not exceed six years of imprisonment and the maximum fine of one million. For example, in the United States for these offenses can be up to 25 years.

Volodymyr Shablystyi, Vitaliy Prymachenko, Anastasiia Filipp, Lina Doroshenko, Vitaliy Burbyka noted that the working body of the National Security and Defense Council of Ukraine in the field of cyber protection is the National Cyber Security Coordination Center, which per the Regulation. One of the priorities of the National Cybersecurity Coordination Center is the measures implemented to ensure the cybersecurity of critical infrastructure facilities and technological processes protection in production in the real economy [20].

In Ukraine, cyberspace is regulated by many different acts. The main of them include the Laws of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", "On Information", "On Telecommunications", "Convention on Cybercrime", as well as the Criminal and Criminal Procedural Codes of Ukraine [21]. These laws give a more excellent definition of all cyberspaces and its levels and regulate specific issues of its functioning. Still, the law on the basic principles of cybersecurity, besides, also establishes the principles and peculiarities of combating cybercrime. The "Convention on Cybercrime" regulates cybercrime issues in detail, especially internationally [11]. The Criminal Code of Ukraine (2001) establishes an exhaustive list of such criminal offenses. As for the Criminal Procedure Code 2010 [22], the issue of cybercrimes is settled quite generally on a part with other criminal offenses, not considering the peculiarities of this phenomenon. In Ukraine today, there is a Cybersecurity Strategy of Ukraine, approved by the relevant Decree of the President. The peculiarity should be noted that cyberspace was equated with a separate area of warfare in its content, on a par with land, air, or sea.

All types of cybercrimes are specified in the Criminal Code of Ukraine, Chapter XVI – Criminal offenses related to the use of electronic computing machines (computers), systems, and computer networks, and telecommunication networks [22].

Article 361 - unauthorized interference with the work of electronic computing machines (computers), automated systems, computer networks, or telecommunication networks. This article involves interference that led to leakage, loss, tampering, blocking information, distorting its processing process, or disrupting its routing [22]. According to Article 361, the most common criminal offenses are hacking or unauthorized modifications of devices or programs. There are many hacking methods, but you can highlight the basics based on others, including its theft and forwarding, which provides access to various devices, systems, and networks. The most common method is Brute force. The spread of computer viruses is another way of hacking based on the distance of malicious programs, which carry out specific work with information, including its theft and forwarding, which provides access to various devices, systems, and networks. Viruses are spread partially legally, first infecting a file that Internet users download themselves to their computers or systems, where the virus itself is activated when the file is started. As a method of hacking, viruses are also universal, but they are also used for several different cybercrimes.

Article 361-1 - creation for use, dissemination, and distribution of harmful software or hardware, as well as their dissemination and distribution [23]. The criminal offenses under this article relate to illegal actions related to malware or technical means. As to the malicious software – it is computer viruses. Viruses are programs that can be independently multiplied and distributed in systems and perform different functions. Viruses hide malicious activity and change processes in the computer system, which facilitates the actions of intruders. Especially dangerous, especially now there are two types of viruses – lockers and miners. Lockers are viruses that block access to computer information or a system and then request to pay for unlocking. Most of these viruses destroy data, and even compliance does not save. The latest known case of such a virus is the Petya virus, which has caused significant damage to both the Ukrainian and Baltic countries. Miners are viruses that began to spread actively after the popularization of cryptocurrency. After penetration into the system, these programs run processes that are aimed at extracting electronic currency, which in turn loads systems very much and impairs the operation of technology.

Article 361-2 - unauthorized dissemination and distribution of information with restricted access stored in the electronic computing machines (computers), automated systems, computer networks, or information-carrying medium [23]. Such illegal actions with information presuppose that they were committed by a person who did not have the right to do so and that access to information was obtained illegally. This article more clearly regulates the issue of information leakage. For example, information is different, official, secret, personal, etc., following which its sale may lead to violations of dispositions of other articles of the Criminal Code. The deal of information is also a special kind of dissemination, which involves commercial intent. Dissemination of information concerns actions that led to its leakage due to which persons who did not have such a right gained access to it.

Article 362 – unauthorized actions with information, processed in the electronic computing machines (computers), automated systems, computer networks, or saved on the information-carrying medium, committed by a person entitled to access such information [23]. This article is very ambiguous, as it provides many possible actions and consequences, and the form of guilt is significant. If such activities are committed intentionally, the products will be like those provided in Article 361 of the Criminal Code, i.e., a leak, loss, forgery, blocking of information, distortion of information processing, or violation of the established routine procedure. Suppose such actions are committed recklessly, such as using a computer to interfere with another computer, etc., which caused significant damage. In that case, the employee should bear the responsibility, not the intruders who spread this virus. Here are questions to the company regarding their methods of protection against malware. The case's resolution depends on many other objective circumstances, despite the subject of these criminal offenses.

Article 363 – a violation of operating rules of electronic computing machines (computers), automated systems, computer networks, or telecommunications networks, and the order or rules protection of information processed therethrough [23]. This article covers actions related to the illegal use of computer electronics, systems, and networks. This mainly applies to activities that are aimed at committing other cybercrimes or criminal offenses using cyberspace. Such actions include, for example, intentional distribution of malicious programs, interference with (hacking) of different devices, systems, or networks, illegal dissemination of information, etc.

Article 363-1 - impeding the work of electronic computing machines (computers), automated systems, computer

networks, or telecommunication networks by mass distribution of electronic messages [23]. As in Article 363, all actions are related to violation of the rules of operation, but Article 363-1 separately allocates specific measures aimed at preventing the functioning of other computer devices; DDoS (dudes) attack is the most common such criminal offenses – actions aimed at overloading a different varnish of cyberspace (computer, site, or server), by exceeding network requests, i.e., overloading the system with information that in turn can slow down or completely fail.

Seemingly, the issue of cybercrimes is sufficiently settled, but the point of counteraction has several serious gaps; to a greater extent, it concerns the imperfection of the criminal process. Today, this legal sphere is actively developing reforms to strengthen the legal support of cybersecurity and counter cybercrimes.

Today in Ukraine, as in the world, the level of cybersecurity is insufficient. Of course, international cooperation contributes to solving this problem. Still, the most critical actions must be taken in the middle of the country to subsequently convey to the world our successful experience of combating cybercrime and regulating cyberspace. To do this, the state and society must join forces and do everything possible to overcome cybercrime. Reforms that continue today are fully justified and are necessary. Still, ideally, the legal sphere should consider the economic and social aspects of cybercrime and technical ones, especially in matters of procedural legislation.

7. MAIN THREATS AND CYBERCRIME PREVENTION IN THE BALTIC STATES AND UKRAINE

Continuous improvement of forms and ways of transnational cybercrimes leads to a systematic approach to counteracting these illegal acts. The European Union pays close attention to countering cybercrime, increasing the resilience of the European Union's cyberspace and other aspects of cybersecurity. According to statistics, 1 million people are victims of internet offenses every day [24].

This research article attempts not only to systematize modern legal norms regulating the cooperation of EU member states in the fight against considered cybercrimes but also to identify the prospects for using tools available in the EU within the standard foreign and security policy framework on countering cybercrime. It should be mentioned that the legal basis for regulating the cooperation of EU member states in the fight against cybercrime is primary (constituent agreements) and secondary EU law (regulations, directives, decisions).

The EU's constituent treaties provide for the general principles of interaction between EU member states in the criminal law sphere. For the first time, harmonization of criminal legislation regulating counteraction to cybercrime was included in the draft Constitution for the EU (Art. III-271). In the future, this provision was also enshrined in the Lisbon Treaty on amendments to the TREATY on the EU and the Treaty establishing the European Community of December 13, 2007 (in the future referred to as the Lisbon Trust).

Currently, detailed regulation of the interaction of states in the fight against cybercrime is carried out through acts of secondary law. To harmonize the criminal legislation of the EU countries, the EU Council adopted: Framework decisions of 22 May 2001 on combating fraud and counterfeiting of non-cash payment means, as well as the Directive of the European Parliament and the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children and child pornography, and replaces the Framework Decision of the Council 2004/68, the Directive of the European Parliament and the Council of August 12, 2013, on attacks on information systems and replaces the Framework Decision of the Council 2005/222.

The Directive on attacks on information systems of August 12, 2013, criminalizes illegal access to the information system, unlawful interference with the design, unlawful influence on data and an illegal interception, illegal use of devices and software, including the creation of botnets the case where the criminal impact on computer data or systems is related to the misuse of another person's data, this may, under national law, be considered an aggravating circumstance if such actions are not covered by the norms enshrining other criminal offenses.

At the same time, the Directive of August 12, 2013, does not cover several criminal acts that may take place on the global information network of the Internet. For example, the issue of harmonization of criminal legislation in intellectual property remains unsettled in EU law. Consequently, the point of convergence of national criminal law in counteracting intellectual property offenses in The Intern became the subject of legal regulation within the EU.

The framework decision of May 22, 2001, to combat fraud and counterfeiting of non-cash payment means contains norms that provide for the need to include in the national legislation criminal offenses related to payment documents, computers, and specially adapted devices (Art. 2-4 of the Framework Solution). Due to the emergence of new ways of committing fraud and counterfeiting of non-cash payment means, a clause on the development of the draft Directive was included in the plan of the Draft European Commission for 2020, which would criminalize socially dangerous acts committed in the process of making online payments, as well as take into account the latest trends in the ways and means of committing fraud using computer equipment (for example, skimming, phishing, and farming).

Directive 2017/541 of the European Parliament and the Council of Europe on the fight against terrorism dated March 15, 2017, defines certain aspects of the fight against terrorism, but at the same time it does not contain norms regarding the definition of the concept of cyberterrorism and methods of countering this phenomenon.

This is due to the debatable concept of "cyberterrorism" and the need to include such a criminal offense in the law. At the same time, this directive provides specific provisions aimed at preventing the use of the global Internet for terrorist purposes: public incitement to commit terrorist criminal offenses (Article 5), measures against provocative content on the Internet (Article 21). It should be noted that specially created bodies carry out the international coordination of cooperation of EU member states in the fight against serious cybercrime affecting the territory of two or more EU member states at the European level: Europol and Eurojust (Articles 85, 88 of the Treaty on the Functioning of the EU).

Eurojust, within its competence, holds special meetings on combating cybercrime and coordinates joint investigation teams' creation to investigate such criminal offenses. Thus, the EU uses a systematic approach to coordinate cooperation between EU member states in the fight against cybercrime, which includes regulating the basics of such interaction in the EU's constituent treaties and accordance with their provisions

- a detailed regulation of such cooperation in the rules and directives of the European Parliament and the COUNCIL of the EU. Currently, EU law contains provisions aimed at harmonizing the legislation of the EU member states in this sphere and providing for a simplified procedure for the interaction of competent authorities of the EU member states to stop, investigate cybercrimes, and bring to criminal responsibility the persons who committed them.

The "European Cybersecurity Strategy" defines the procedure for responding to different types of cyberincedenters. Thus, following paragraph 3.2 of this act, if cyberintsident is a criminal offense, it is reported by Europol and the European Cybercrime Centre to react to it together with the competent authorities of the EU Member States. At the same time, an EU member state can appeal to Art. 222 of the Treaty "on the Functioning of the EU" if the incident: a) refers to cyberespionage or attack sponsored by the state or has implications for national security; b) is particularly dangerous.

Note that the EU uses a systematic approach to coordinate the cooperation of member states in the fight against cybercrime, which has a legal and institutional component. It was found that the specifics of the content of secondary law acts regulating the cooperation of EU member states in the fight against cybercrime are that they:

a) aimed at harmonization of criminal legislation in this sphere.

b) regulate international cooperation in the fight against such criminal offenses.

c) establish a simplified procedure for prompt interaction of competent authorities using such tools as a European warrant for investigation, a European arrest warrant.

At the same time, there is currently no legal basis in the EU to harmonize the criminal legislation of the EU Member States in the fight against cybercrimes in the field of intellectual property; 22 May 2001 to combat fraud and counterfeiting of non-cash payment means [25]. All this shows the need to improve further the legal regulation of cooperation in the fight against cybercrime within the EU.

8. INTERNATIONAL LEGAL COOPERATION PECULIARITIES IN THE FIGHT AGAINST CYBERCRIME WITHIN THE EUROPEAN UNION

The rapid development of information technology and the informatization of society has led to the emergence of new types of criminal offenses and threats - such as cybercrime, cyberterrorism, cyber warfare. The Russian Federation has been pursuing an information policy to form a negative image of the Baltic States on the international stage for a long time. According to the comparative analysis of Russian-language content in the information space of the Baltic countries, in addition to employees of mass communication, well-known Russian research institutions and some representatives of the scientific public are also involved. In particular, the annual report of the Latvian Security Police for 2017 shows the strengthening of the activities of the Russian special services in the Russian-speaking environment under the slogan of protecting the rights of compatriots. This trend persists in the following 2017-2018: the report for 2019 shows a high level of activity of the Russian special services interest in the country's security and defence issues, social processes, NATO activities in Latvia, relations between individual ethnic groups, etc. Also, Latvian special services once again observe a noticeable intensification of activities in the Russian-speaking youth environment.

In the Yearbook of the Estonian Information Department "International Security and Estonia", it is alleged that the Russian Federation carries out information campaigns against NATO member states and the EU by disseminating destructive information through the media and social networks. "Russia consistently spreads the thesis that Estonia, Latvia, and Lithuania do not respect the rights of its Russian-speaking residents and falsify history. Baltic countries create the image of undemocratic and problematic partners to weaken their connection with allies and reduce their role in shaping foreign policy towards Russia.

The report of the Department of State Security of Lithuania for 2017 refers to the dissemination of information inappropriate for this state, intelligence from the territory of the Russian Federation and the Republic of Belarus (in the future - the Security Council), aimed at the military and other infrastructures of the country, electronic intelligence, and cyber spying.

Summing up the fore, we note that the main threat to the national security of the Baltic states is the propaganda activities of the Russian Federation in the information sphere and its destructive activities in the information space. Russian scientists' repeated attempts to rewrite the history of the Baltic states, falsification and propaganda resemble the Russian scenario on the eve of the annexation of the Crimean Peninsula and military aggression in eastern Ukraine.

To prevent cybercrimes, it is necessary to comprehend this phenomenon. The issue of combating cybercrime is overly complex and ambiguous due to many features. This process should include not only the state but also civilian activities to achieve the goal. It is worth noting that the legislation on cybersecurity of both the Baltic states and Ukraine determines that cybersecurity subjects are government agencies and non-governmental organizations, and other individuals and legal entities.

Speaking of the role of non-governmental organizations and society in combating cybercrime, their primary role is the prevention of cybercrimes by creating more secure cyberspace. The main task of humanity is caution. Users of modern technologies must comply with all necessary rules of conduct on the network, including the use of protective software and legally licensed software, careful use of Internet resources, control over personal data on the web, etc. In addition to increasing the overall level of network security, it can also help reduce the number of emerging cybercriminals, and the caution of cyberspace users will complicate their activity [26].

Because the information technologies that exist now allow both to hide the location and use the data of others, we believe that the following steps should be taken to ensure the prevention of cybercrimes in the Baltic states and Ukraine. Internationally, in our opinion, it is worth it:

- to develop and implement international agreements in the field of prevention and investigation of cyberaggression.

- to create an international body with regional offices. This body should be the UN equivalent in cyberspace. In our opinion, it will be advisable to function within such a body of certain levels. The performing group maybe, in our opinion, internationally, regionally, and at the national level. The regional level will allow, in case of cyberaggression, to be included in the counteraction in time, the national level will allow on a par with local, national representatives to include regional and international representatives of the said

international organization in the investigation [27].

At the national level, each of the countries considering offers:

- participate in the development of an international strategy to counter cyber threats and create unified international legal mechanisms for regulating virtual space;
- to develop a draft National Concept of the State Cybersecurity Strategy, which should be based on the principles and laws of other government documents that would consider its implementation at different national levels and spheres;
- increase capacities in the information sphere on countering electronic attacks. It is necessary to strengthen measures of a domestic political nature to stimulate the development of the technological component of cybersecurity to maintain the balance of power and to draw up a counterweight to other prob ask "adversaries" in the field of cybersecurity;
- to advocate, implement and implement regional, international cooperation in the field of cybersecurity, tracking the activities of criminal, terrorist groups, and individual hackers operating in cyberspace;
- to advocate and actively participate in the development of international cooperation in the region and structures aimed at detecting cyber threats, timely detection, prevention, protection, as well as minimization of consequences;
- to develop and implement a multilevel institutional cybersecurity system. In our opinion, such a system should include: a scientific and analytical level that would study cybersecurity risks by the possibilities of implementing cyber threats and the size of negative consequences; would actualize the means and methods of ensuring cybersecurity and a qualifying level that would coordinate at the internal and external groups.

The main directions of countering cybercrime are to solve problems related to the expansion of legislation, developing measures to prevent and reduce the level of latency of criminal offenses carried out in cyberspace. However, today, in the face of the challenges and threats of the XXI century, it is necessary to discuss and solve the problems that new technologies pose to criminal policy.

9. CONCLUSIONS

The annual flow of cybersecurity incidents is increasing year by year, becoming steadfast as deaths and taxes. And this tendency does not change, despite all the efforts of cybersecurity professionals, corporations, government, agencies, scientists, and "white hats" around the world. At the same time, the flow of publications on cybersecurity has increased significantly in recent years, including research reports that predict to some extent the global cybersecurity landscape, which allows us to build a positive outlook.

It can be noted the tremendous social danger of cybercrime in the period of its formation and development. Although there were no intelligent systems of information protection, the criminal offenses themselves were primarily expressed in external contact with information repositories (to commit illegal interference, copying, alteration of information). Currently, there is a high relevance and public danger of cybercrime. This crime has a high degree of latency, can be expressed in the commission of "traditional" illegal acts (but in the field of cyberspace or with the use of cyber technology) and significant complexity of directions (in particular, we mean the difficulty of finding criminals and compensation). Besides, there was a third factor - immensity, etc. Cybercrime can occur wherever there is the Internet, network structures, or information technology. That is why it is vital to ensure an effective and optimal criminal policy in the fight against this type of crime at the international level.

The authors would like to point out that despite the fact that Ukraine and the Baltic States have ratified the Convention on Cybercrime, the real implementation of the Convention's norms in the legislation of the states has not taken place. Each of the considered countries implemented only the norms on crimes in the field of use of electronic - computing machines, where the object of encroachment is computer information. At the same time, leaving other cybercrimes practically unregulated in the criminal legislation of these countries, in particular, "phishing", "carding", "spam", etc. In addition, the authors observe that the sanctions of certain articles related to cybercrimes are very loyal and in the vast majority provide punishment in the form of a fine. Therefore, it would be more expedient to take measures to strengthen the sanctions of such articles.

Thus, we believe that to combat criminal offenses committed with the use of modern information technologies in our country should constantly increase the security of information systems, develop modern information technologies, improve legislation in the field of information criminal offenses, develop competitive means of information, expand international cooperation use of information resources.

REFERENCES

[1] Furashev, V.M. (2012). Cyberspace and information space, cyber security and information security: Essence, definition, differences. Information and Law, 2(5): 162-175.

[2] Korobeev, A.I., Dremlyuga, R.I., Kuchina Ya, O. (2019). Cybercrimes in the Russian Federation: Criminological and criminal law analysis of the situation. Vserossiiskii kriminologicheskii zhurnal= Russian Journal of Criminology, 13(3): 416-425. https://doi.org/10.17150/2500-4255.2019.13(3).416-425

[3] Report of the X UN Congress on the prevention of crime and the treatment of offenders. (2000). https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-EN.pdf.

[4] EC. (2012). Communication from the commission to the European parliament, the council and the committee of the regions. https://www.eea.europa.eu/policy-documents/communication-from-the-commission-to-1.

[5] Clough, J. (2011). Data theft? Cybercrime and the increasing criminalization of access to data. Criminal Law Forum, 22(1): 145-170. https://doi.org/10.1007/s10609-011-9133-5

[6] Khusyainov T. (2015). Internet crimes (cybercrime) in the Russian criminal legislation. In the collection: criminal law of the Russian Federation: Problems of law enforcement and prospects of improvement material soft heal –Russian round table. https://publications.hse.ru/pubs/share/folder/t0d29dcc24/186300253.pdf.

[7] Leukfeldt, E.R., Lavorgna, A., Kleemans, E.R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial

cybercrime as organised crime. European Journal on Criminal Policy and Research, 23(3): 287-300. https://doi.org/10.1007/s10610-016-9332-z
[8] Nomokonov V., Tropina T. (2012). Cybercrime as a new criminal threat. Yesterday, Today, Tomorrow, 24: 47. https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza.
[9] Karpova, D. (2014). Cybercrime: A global problem and its solution. Can.,8: 46-50. https://cyberleninka.ru/article/n/kiberprestupnost-globalnaya-problema-i-ee-reshenie/viewer.
[10] https://konference.nvsu.ru/konffiles/331/XX%20stud%20conf%20NVSU_2018_Ch%202_Inform.%20tech.,%20mathem.pdf, accessed on June 19 2022.
[11] https://www.refworld.org/docid/47fdfb202.html, accessed on June 19 2022.
[12] Goodman, M.D., Brenner, S.W. (2002). The emerging consensus on criminal conduct in cyberspace. International Journal of Law and Information Technology, 10(2): 139-223. https://doi.org/10.1093/ijlit/10.2.139
[13] Ilchenko, O., Chumak, V., Kuzmenko, S., Shelukhin, O., Dobrovinskyi, A. (2019). Fishing as a cybercrime in the internet banking system: economic and legal aspects. Journal of Legal, Ethical and Regulatory Issues, 22(2): 1-6.
[14] Global Cybersecurity Agenda (GCA). (2007). https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx, accessed on June 19 2022.
[15] https://wiselawyer.ru/poleznoe/73666-kompyuternoe-moshennichestvo-byli-osnovaniya-kriminalizacii, accessed on June 19 2022.
[16] Newmeyer, K.P. (2015). Elements of national cybersecurity strategy for developing nations. National Cybersecurity Institute Journal, 1(3): 9-19.
[17] https://www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas_strategija%20EN%20%281%29.pdf, accessed on June 19 2022.
[18] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf, accessed on June 19 2022.
[19] https://cyberpolice.gov.ua/results/2018/, accessed on June 19 2022.
[20] Shablystyi, V., Prymachenko, V., Filipp, A., Doroshenko, L., Burbyka, V. (2019). Legal principles of cyber protection of critical infrastructure facilities. Journal of Legal, Ethical and Regulatory Issues, 22(6): 1-6.
[21] https://minjust.gov.ua/m/str_24640, accessed on June 19 2022.
[22] Review of the Bulletin of the VRU. Retrieved from: https://zakon.rada.gov.ua/laws/main/4651-17, accessed on June 19 2022.
[23] http://zakon3.rada.gov.ua/laws/show/2341-14, accessed on June 19 2022.
[24] https://research.utwente.nl/en/publications/towards-eu-cybersecurity-law-regulating-a-new-policy-field, accessed on June 19 2022.
[25] Мороз, Н.О. (2018). Особенности международно-правового сотрудничества в борьбе с киберпреступностью в рамках ЕС. Вестник Марийского государственного университета. Серия «Исторические науки. Юридические науки», 4(16): 87-94. https://doi.org/10.30914/2411-3522-2018-4-4-87-94.
[26] Holub, A. (2016). Cyber crime in all its events: types, consequences and methods of combating. Bezpechne misto. https://www.gurt.org.ua/articles/34602/, accessed on June 19 2022.
[27] Chowdhury, N., Nystad, E., Reegård, K., Gkioulos, V. (2022). Cybersecurity training in Norwegian critical infrastructure companies. International Journal of Safety and Security Engineering, 12(3): 299-310. https://doi.org/10.18280/ijsse.120304