DOI: https://doi.org/10.34069/AI/2021.38.02.10

Cybercrime: History of formation, current state and ways of counteraction

КІБЕРЗЛОЧИННІСТЬ: ІСТОРІЯ ФОРМУВАННЯ, СУЧАСНИЙ СТАН ТА ШЛЯХИ ПРОТИДІЇ

Received: February 12, 2021 Accepted: March 5, 2021

Written by:
Viktoria Babanina[26]
https://orcid.org/0000-0003-4173-488X
Iryna Tkachenko[27]
https://orcid.org/0000-0002-0144-0708
Olena Matiushenko[28]
https://orcid.org/0000-0003-1507-2085
Mykola Krutevych[29]
https://orcid.org/0000-0001-5432-9256

Abstract

The article examines the history of the emergence and development of cybercrime, the specifics of the current situation in society, which contributes to an increase in the number of cybercrimes and ways of countering cybercrime. It has been established that cybercrime first appeared in the middle of the last century. This was due to the emergence and subsequent intensive growth in the number of computers, and then smartphones. However, cybercrime that exists today is significantly different from what it was in its early days. Today, the number of devices and services provided via the Internet is growing, the number of users is growing, and, accordingly, the number of cybercrimes and the level of their organization is growing. In the course of the study, the differences between the concepts of "cybercrime" and "computer crimes" were identified, as well as the main features of cybercrimes. The problems that law enforcement agencies face in the investigation and fight against cybercrimes were revealed. The factors contributing to the growth of cybercrime were also analyzed. Based on the analysis, the main directions of combating cybercrime and preventing the growth of the number of cybercrimes in society were developed.

Анотація

У статті розглядається історія виникнення та розвитку кіберзлочинності, особливості сучасної ситуації в суспільстві, що сприяє збільшенню кількості кіберзлочинів та шляхи протидії кіберзлочинності. Встановлено, що кіберзлочинність вперше з'явилася в середині минулого століття. Це було пов'язано з появою та подальшим інтенсивним зростанням кількості комп'ютерів, а потім і смартфонів. Однак кіберзлочинність, яка існує сьогодні, суттєво відрізняється від тієї, що була в її перші дні. На сьогоднішній день зростає кількість пристроїв та послуг, що надаються через Інтернет, зростає кількість користувачів, і відповідно зростає кількість кіберзлочинів та рівень їх організації. В ході дослідження було виявлено відмінності між поняттями «кіберзлочинність» та «комп'ютерні злочини», а також основні ознаки кіберзлочинів. Були розкриті проблеми, з якими стикаються правоохоронні органи під час розслідування та боротьби з кіберзлочинами. Також були проаналізовані фактори, що сприяють зростанню кіберзлочинності. На основі проведеного аналізу розроблено основні напрямки боротьби з кіберзлочинністю та запобігання зростанню кількості кіберзлочинів у суспільстві.

[26] Professor of Criminal Law Department of the National Academy of Internal Affairs, PhD in Law, Associate Professor, Kyiv, Ukraine.
[27] Lecturer of Criminal Law Department of the National Academy of Internal Affairs, PhD in Law, Kyiv, Ukraine.
[28] Acting Head of Department of Criminal Law of National Academy of Internal Affairs, PhD in Public administration, Kyiv, Ukraine.
[29] Lecturer of Criminal Law Department of the National Academy of Internal Affairs, Kyiv, Ukraine.

Key Words: computer crime, countermeasures, cybersecurity, cybercrime, information society.

Ключові слова: комп'ютерна злочинність, контрзаходи, кібербезпека, кіберзлочинність, інформаційне суспільство.

Introduction

At the present stage of formation and development of the information society, the process of digitalization is global, comprehensive, penetrating into all spheres of public life. It is becoming one of the main factors of social development and largely characterizes modern social dynamics. Due to the process of informatization of society there are systemic changes, according to which all segments of society and each person are included in the global information space, becoming elements of the global information system and, accordingly, to some extent dependent on it.

This information dependence applies to the world as a whole, all states and people involved in the production, storage and use of information in the course of information exchange and information interaction. Information interaction has already become a planetary factor, creating a number of social transformations and introducing into the system of social relations such processes as information wars, information weapons, information terrorism, information crime and information security so on.

Modern social practices show that social development on the basis of global informatization creates qualitatively new challenges, threats and risks of information security. This fact makes the study of information security relevant.

In the process of information globalization a single information space has been created, which led to the unification of information technologies of all countries. The emergence of a global information space inevitably causes a change in the elements of the legal system. Along with traditional institutions, new ones are emerging due to the development of information and communication technologies. The development of information technology also poses a significant threat, in cases where they are used to the detriment of society, in order to cause harm. In such cases, we are dealing with a new type of crime - cybercrime, which requires the study, analysis and development of countermeasures.

It is known that the issues of information security, protection of computer information, ensuring the protection of information that constitutes a legally protected secret, and other similar issues are of serious concern both in Ukraine and around the world. These issues are directly related to ensuring the national security of states, protection of human constitutional rights and freedoms. The need to combat crimes in the field of information technology is confirmed by the fact that recently these crimes have become a global international problem, many of these crimes are cross-border in their nature.

Research background

The study of scholars' works reveal that at the moment there is a large number of researches that address some aspects of the fight against cybercrime. In particular, the works of F. Almenar Pineda (2020), D. Azarov (2007), Yu. Baturin (1991), P. Bilenchuk & T. Obihod (2018), C. Brants et al. (2020), V. Butuzov (2010), Ye. Hong & W. Neilson (2020), V. Stets (2019), Tamarit J.M. (2020), T. and others are devoted to this issue.

Among mentioned works a very important role in understanding of the meaning and specifics of computer crimes plays the work of D. Azarov (2007), who was one of the first scholars in Ukraine to research this notion. In his monograph, he explored the problems of criminal liability for crimes in the field of computer information, the degree and public danger of such encroachments, their international nature. The scientist also summarized the international experience in the fight against computer crime and proposed on the basis of his analysis significant changes in Ukrainian legislation. Yu. Baturin (1991) was one of the first scholars to research the situation on computerization and computer crimes in the post-soviet space. His monograph was devoted to the development of legal support of computer science in the USSR, taking into account foreign experience and global trends in computerization of society. It addressed issues related to the legal regime of machine information, mandatory relations in the field of computer science, security of computer facilities, computer crimes and their prevention, the use of computers in the application of law, the impact of computerization on the law of military conflicts. V. Butuzov in his monograph

"Counteraction to computer crime in Ukraine" (2010) defined the concept of computer crime, its types and features, as well as proposed methods of their investigation. V. Stets (2019) has made a significant contribution to defining the essence of cybersecurity. In particular, he identified the place of cybersecurity in the structure of national security of Ukraine and its correlation with information security, analyzed approaches to defining the essence of cybersecurity and proposed his own definition of cybersecurity.

Tamarit, J.M. (2020) in their research article mention that one of the main problems in preventing and prosecuting cybercrime is insufficient reporting Scholars emphasize the need to implement specific mechanisms to facilitate the reporting of cybercrime and ensure that the rights and needs of victims are properly addressed. Brants C., Johnson D. and Wilson T. (2020) considered the possibility to apply familiar criminal justice issues or dilemmas to the exponential increase in cybercrime and whether functional adaptation was successful. Hong Ye. and Neilson W. (2020) investigated cybercrime by adding an active victim to Becker's basic crime model. Almenar Pineda F. (2020) studied how technological progress and the digitization of information had affected modern society and put significant risks to human freedoms, even to the rule of law.

Despite the relatively large number of publications, the issue of combating cybercrime remains poorly understood and requires further comprehensive research. It is especially relevant taking into account recent changes in legislation on this issue.

Methodology

The choice of research methods was determined by the purpose of the study, which is to study the essence of cybercrime and measures to combat cybercrime. To achieve this goal, the following tasks were solved: to study cybercrime as a phenomenon, to study the preconditions of its origin, development; to study experience in the field of combating cybercrime; to explore the nature and features of cybercrime; to provide recommendations on a cybercrime prevention.

Given this, the methodological basis of the study is based on the use of a dialectical method of studying social processes and phenomena. The nature of the research tasks determined the need to use such methods as comparative-historical, comparative-legal, method of systematic analysis and specific-sociological method.

The historical method in the study was used to study the history of the emergence and development of cybercrime in the world. Using formal-logical and dogmatic methods, modern norms of cybercrime and approaches to defining the concept of cybercrime were analyzed. The comparative-legal method was used to identify the specifics of cybercrimes in relation to other types of crimes, as well as to determine the characteristic features of cybercrimes. The development of ways to counter cybercrime was carried out using dialectical and formal-logical methods.

Results and discussion

The paradox of human development is that throughout their development people have used, accumulated, transmitted information. The continuous process of informatization of society covers all areas of human activity and the state: from solving problems of national security, health care and transport management to education, finance, and even interpersonal communication. With the development of electronic payment technologies, "paperless" document management, a serious failure of local networks can paralyze the work of entire corporations and banks, which can lead to significant material losses.

The history of cybercrime is the latest story that concerns us all. Currently, the problem of cybercrime has grown into a global community.

The term "cybercrime" is now often used alongside with the term "cybercrime", and often these terms are used interchangeably. Indeed, these terms are very close to each other, but still not synonymous (Pogoretsky, 2012). The concept of "cybercrime is broader than "computer crime", and more accurately reflects the nature of such a phenomenon as crime in the information space. Thus, the Oxford Dictionary (2021) defines the prefix "cyber-" as a component of a complex word. Its meaning - "connected with electronic communication networks, especially the internet". Thus, "cybercrime" is a crime related to the use of electronic communication networks and the use of information technology. At the same time, the term "computer crime" refers only to crimes committed against computers or computer data.

According to UN experts, the term "cybercrime" covers any crime that may occur through a computer system or network, within a computer system or network, or against a computer system or network (United Nations, 2000). Thus, cybercrime can include any crime committed in an electronic environment.

A crime committed in cyberspace is an illegal interference in the work of computers, computer programs, computer networks, unauthorized modification of computer data, as well as other illegal socially dangerous acts committed with the help of computers, computer networks and programs (United Nations, 2000).

Today, cybercrime is a large-scale problem, and malware is written for the purpose of illegally obtaining money. The development of the Internet has become one of the key factors that determined these changes. Companies and individual users can no longer imagine their lives without it, and more and more financial transactions are conducted via the Internet. Cybercriminals have realized the enormous potential for "making" money with malicious code in recent times, and many of today's malware is written to order or for resale to other criminals.

The Council of Europe Convention identifies four types of computer crimes, which are defined as crimes against the confidentiality, integrity and accessibility of computer data and systems (Council of Europe, 2001):

1) illegal access - Art. 2 (illegal intentional access to a computer system or part thereof);
2) illegal interception - Art. 3 (unlawful intentional interception of non-public transmissions of computer data to a computer system, from it or within it);
3) data interference - Art. 4 (unlawful damage, deletion, violation, alteration or termination of computer data);
4) system interference - Art. 5 (serious unlawful interference with the operation of a computer system by entering, transmitting, damaging, destroying, disrupting, altering or terminating computer data).

In addition to the transformation of cybercrime itself, the characteristics of the hacker are also changing: if at first it was people who had the knowledge, skills, who directed their actions not so much to illegal goals, but to find new ones, now behind criminal activity is the criminal business. There is a stratification of attackers into people who have high knowledge in this specific area, which can be classified as "elite", and people who have received a ready-made algorithm that ensures the implementation of a certain procedure, while having a very general idea of the processes occurring in information systems (Council of Europe, 2001).

The first category of cybercriminals, namely they pose the greatest threat today, has quite characteristic, pronounced features. These include:

– ability to commit criminal acts anonymously, secretly;
– criminal acts are best in the cross-border jurisdiction of different states;
– high professional and intellectual abilities of a hacker;
– the possibility of combining disparate computers into a single mechanism for committing criminal acts in an automated mode;
– absence, or long-term temporary delay of the victim's awareness of the fact of committing criminal influence;
– the presence of a large number of victims of a hacker attack;
– no need for the hacker to come into direct contact with the victim of his illegal action.

The emergence of cybercrime can be counted from the advent of the computer, the so-called computer age. The history of cybercrime can be divided into two periods: the first - from the creation of the first computer to 1990 and from 1990 to the present. The fact is that since 1990, the Internet has begun to spread around the world with great speed (Nekit, Ulianova & Kolodin, 2019).

The first mention of using a computer to commit a crime was made public in the 1960s, when computers were large universal computers. After World War II in 1946, several companies began working on commercial computers and by 1951 UNIVAC was producing the first commercial computer created in the United States and the third commercial computer in the world, which was not intended for use in weapons development research. A total of 46 UNIVAC copies were created between 1951 and 1958. They were installed in government agencies, private corporations and in three US universities (Gritsyak, 2015).

Electronic vacuum lamps emitted a lot of heat, absorbed a lot of electricity, were bulky, expensive and unreliable. First-generation

computers built on vacuum tubes had low speeds and low reliability.

In 1947, the employees of the American company "Bell" William Shockley, John Bardin and Walter Brettein invented the transistor. Transistors performed the same functions as electronic lamps, but used the electrical properties of semiconductors. Compared to vacuum tubes, transistors took up 200 times less space and consumed 100 times less electricity. At the same time, there are new devices for organizing computer memory - ferrite cores. With the invention of the transistor and the use of new technologies for storing data in memory, it became possible to significantly reduce the size of computers, make them faster and more reliable, as well as significantly increase the memory capacity of computers (Dovgan, 2018).

In 1954, Texas Instruments announced the start of mass production of transistors, and in 1956, scientists at the Massachusetts Institute of Technology created the first fully built on transistors computer TX.

In the 60's of last century there was a third generation of computers, which for the first time began to use integrated circuits (chips). At the same time, there is a semiconductor memory, which is still used in personal computers as RAM. During these years, the production of computers is gaining industrial scale. IBM was the first to implement a family of computers - a series of fully compatible computers from the smallest, the size of a small closet (less then not yet made), to the most powerful and expensive models.

Back in the early 60's, the first minicomputers appeared - small low-power computers, available at a price to small firms or laboratories. Minicomputers were the first step towards personal computers, prototypes of which were released only in the mid-70's. Along with the rapid development of the computer sphere, cybercrime begins to develop (Dovgan, 2018).

But cybercrime in the 1960s and 1970s was different from cybercrime today. First, at that time the Internet had not yet appeared, and secondly, computers were not integrated into a network. In 1960, a typical computer cost several million dollars, took up one room and required a special air conditioning system to keep the computer from burning. At that time, only a certain circle of researchers and scientists could use computers in their work.

Limited use of computers and lack of connection to other computers dramatically reduced the chances of committing computer crimes, and if they occurred, then only people who serviced computers. All crimes of that time were reduced to crimes related to financial investments in computers. This lasted until the emergence and worldwide spread of the Internet, which opened up new opportunities for criminals (Dovhan & Tkachuk, 2018).

The history of cybercrime can be considered in the history of hacking. A hacker is a highly qualified IT specialist, a person who understands the intricacies of computers. There are two types of IT-hackers: "White hat" and "Black hat". "Black hat" refers to cybercriminals, while "White hat" - other information security professionals (including professionals working in large IT companies) or IT researchers who do not break the law (Moiseev, 2016).

The second stage in the development of cybercrime dates back to the mid-1990s, a period when the Internet was spreading at a rapid pace. It was a time when personal computers and the Internet became more widely available. In December 1995, an estimated 16 million Internet users were registered worldwide, and by May 2002, that number had risen to 580 million, or nearly 10 percent of the world's population (Yar, 2015). It should be noted that the spread of the Internet around the world was uneven, for example, more than 95 percent of the total number of Internet connections were located in the United States, Canada, Europe, Australia and Japan. It was at this time that a new type of crime, called "hacking," was introduced into the history of crime.

At the initial stage of development of cybercrime, the term "hacking" is very often used, although later hacking will be defined as one of the crimes included in the concept of cybercrime. It is the hacking that characterizes the illegal actions of hackers.

Cybercrime is not only a technical and legal, but also a social problem, the effective solution of which requires, above all, a systematic approach to developing a framework for ensuring the security of vital interests of citizens, society and the state in cyberspace.

According to the mechanisms and methods of committing a crime in the field of computer technology, they have a high level of latency. The greatest public danger is posed by crimes

related to unauthorized access to computer information.

The analyzed offenses have a very high latency, which, according to various data, is 85-90%. Moreover, the facts of detection of illegal access to information resources by 90% are random (Pozhuyev, 2016).

These data suggest that law enforcement officials often simply do not understand how to investigate these crimes and how to prove them in court. Hence, the inability to conduct quality investigations, traditional methods of organizing and planning investigations do not work in these conditions, it is necessary to increase the efficiency of law enforcement, increase the level of demand for the level of professionalism of law enforcement officers, their moral and business qualities. Their formal attitude to reporting the results of the fight against cybercrime should not be allowed.

Another problem that scholars most often face when investigating computer crimes is to establish the fact of the crime. This is due to the fact that computer crimes are often committed in the so-called "cyberspace", they know no boundaries, very often crimes are committed without leaving home, using your personal computer (Nekit, 2020). In addition, illegal copying of information often goes unnoticed, the introduction of a virus into a computer is usually attributed to an unintentional mistake of the user who could not "catch" it when in contact with the outside computer world. Also, the attitude of the victims to the encroachment against them is not always adequate. Instead of informing law enforcement about the illegal interference with the computer system, the victims are not willing to do so, fearing that their business reputation will be undermined. Usually, the victims of computer crimes are local networks, servers, individuals (Rogovets, 2015).

It should be emphasized that professional computer criminals choose the local networks and servers of large companies as the object of the crime, in turn, "amateurs" encroach on the information of individuals' computers and less often "hack" Internet service providers, usually for "free" Internet access.

It is noteworthy that the injured party, represented by large corporations that own the system, is reluctant to report (if reported at all) to law enforcement agencies about the facts of a computer crime. And since they make up the majority, this explains the high level of latency of computer crimes.

In addition, officials whose responsibilities include computer security are often not interested in disclosing the fact of a crime. Recognition of unauthorized access to their jurisdiction calls into question their professional qualifications, and the failure of management's computer security measures can cause serious internal complications.

Bank employees usually carefully conceal the crimes they have committed against the bank's computers, as this can have a detrimental effect on the bank's prestige and lead to the loss of customers. Some victims are afraid of a serious competent investigation, because it can reveal obscene or even illegal business mechanics.

There is another problem with the effectiveness of investigating computer crimes and bringing them to justice. This is a public opinion that does not consider computer crimes to be a serious crime due to the fact that computer criminals, even if the investigation is completed and a court sentence is handed down, are punishable by light sentences, often suspended sentences. Hence - legal nihilism, on the one hand, criminals who feel impunity, and on the other hand, victims who do not want to apply to law enforcement agencies for unauthorized access, because they understand that there will be no appropriate punishment for criminals.

Today, active implementation of information technologies in all spheres of activity has led to change of the list of crimes relating to economic. These crimes began to include computer crimes that harm the economy of the state, its individual sectors, business activities, as well as the economic interests of certain groups of citizens. According to experts, in the United States, the annual losses of corporations from crime exceed 200 billion, and from computer crimes - 6 billion dollars. In the UK, computer crimes cost £ 2 million per day (Djerf-Pierre, 2018).

According to a number of studies, every second in the world 12 people become victims of cybercriminals and this number is growing every year (Djerf-Pierre, 2018). We can identify the following factors that affect the growth of cybercrime:

– global informatization of all spheres of society does not increase, but reduces the degree of its security;

- acceleration of scientific and technological progress increases the likelihood of criminals using purely peaceful technologies as a means of destruction, and the possibility of their "dual" use is often not only not foreseen, but also not realized by the creators of technology;
- terrorism is increasingly becoming a special type of information technology, because: first, terrorists are using the capabilities of modern information systems for communication and information gathering; secondly, the reality of our time is the so-called "cyberterrorism"; thirdly, most terrorist acts are now designed not only to cause material damage and threat to human life and health, but also to information and psychological shock, the impact of which on large masses of people creates a favorable environment for terrorists to achieve their goals;
- "digital inequality" and the emergence of countries that have lost the information race can lead to terrorist activity against individual states as a means of asymmetric response.

Subjects of crimes that actively use high technology, along with persons who perform professional functions in organizations and enterprises, are almost any person. At the same time, their purpose, methods used and available opportunities are practically indistinguishable from those inherent in criminals by type of employment. The main motive of cybercriminals is to obtain material benefits.

Cybercriminals use their arsenal of information weapons, which is a set of tools designed to violate (copy, distort or destroy) information resources at the stage of their creation, processing, distribution and storage. The main types of information weapons include the following:

- backdoor - this tool provides a hidden method in the system that allows access to the protected area;
- computer "viruses" - special programs that are embedded in computer software, destroy, distort or disrupt its operation. They are able to be transmitted over communication lines, data networks, disable control systems, etc. In addition, "viruses" are able to reproduce themselves;
- "logic bombs" - software embedded devices that are pre-implemented in the information and control centers of the infrastructure to signal them or at a set time to activate them;
- software products such as "Trojan horse" - programs or utilities that, after installation, perform the declared functions in the background;
- neutralizers of test programs that ensure the preservation of natural and artificial defects of the software;
- traffic analyzers (sniffer) - programs or devices that monitor data transmitted over the network. Traditionally used for legitimate network management functions, they can also be used during cyberattacks to steal information;
- DDos-attacks - designed to disrupt network access, usually by executing millions of requests every second, resulting in network access is difficult or disrupted;
- E-mail Spoofing is a method of sending e-mail with a source substitution, used to force the recipient to provide confidential information;
- Keylogger is a software or hardware that is designed to control the keystrokes on a computer keyboard, to obtain a password, PIN or other information (Europol, 2016).

Due to the availability of Internet services via mobile devices, the use of the Internet is steadily increasing (Statista, 2018). Smartphones are becoming less expensive and include more features, and mobile service providers are providing more reliable Internet access through less expensive cellular networks. This is increasing the penetration of the Internet in many countries.

As the reliability of Internet access increases and the number of people connected to the Internet increases, the number of important services provided online increases. Hundreds of millions of users turn to online services such as instant messaging, online payments, online shopping, online food delivery or online travel booking.

Mobile devices, mobile Internet are so popular that public services, payments, investments, public and private transport and many other services are fully integrated with them. With critical services increasingly offered online, and sometimes accompanied by a reduction in the number of offline services, there are also increasing opportunities for technology abuse and crime

It should be noted that not all cases of violations of legislation in the field of information

technology or with the use of new generation technical devices are aimed at enrichment. Thus, with some probability, we can assume that many criminals in the information sphere use their exceptional skills to make a living, but most often, hacking, disclosure of confidential data is associated with the attempt of information activists to influence public opinion, change the course of political processes. to convey a message to the masses or to spread a certain idea.

One striking example of this kind of crime is the attack on diplomatic and political information networks around the world in 2009, when, first of all, several computers located in the office of the Tibetan government and personally the Dalai Lama were attacked, the operation was carried out using several devices located in the United States and China. According to experts, the purpose of the attackers was to gain access to classified information, espionage and access to video cameras and audio microphones from countries and non-governmental organizations around the world. The operation was called “the Dalai Lama under the hood”.

Another striking example is the cyberattack carried out on the information networks of the United States Democratic Party in 2016, when, due to interference in the work of systems and servers of the National Committee, on the site "Wikileaks", personal letters were published, as well as other digital content intended for internal use by party representatives. This information, according to researchers, could have undermined the trust of voters among the candidate from the Democratic Party of the United States, and directly affect the results of the vote.

Moreover, the course of these elections, as researchers and the media reflect, could have been influenced in the same way by Internet propaganda, with the posting of fake news and investigations (Tench & Yeomans, 2016). The crimes mentioned in the study only partially reflect the general trend of increasing penetration, illegal access, hacking and use of information networks of governments, government agencies, organizations, foundations, etc. in order to change the political situation, to convey a certain position, to influence political processes.

Conclusions

The phenomenon of cybercrime is not new to modern science, although it requires further study, especially in matters of accuracy and definition of the concept.

The main characteristics that distinguish this type of offense from other crimes: high probability of concealment of data, difficulties in the investigation, due to limited information, the impossibility of unification of national laws and approaches to investigation in this area, difficulties in data collection, crime and etc. There is a tendency to increase the impact of such an aspect as the cross-border nature of these offenses.

External threats to cyberspace include hacker attacks carried out from the territories of other states, aimed at disrupting the operation of computer systems, theft of confidential information, and others.

The fight against cybercrime must be systemic in nature, based on current risks and challenges in cyberspace, and the institutional environment for cybersecurity must be constantly improved. The effectiveness of measures in this area should be achieved through the assessment of the threats of organized cybercrime, which will identify current threats and risks in cyberspace. In today's globalized world, Ukraine needs to create an adequate cyber security system.

It should be noted that in the fleeting course of public life, with revolutionary processes in the development of information technology, much of the current regulations, both domestic and international, gradually loses relevance, compliance with the processes they regulate, and needs clarification or revision. The development of information activities creates the need for legal regulation of new aspects of this activity.

Needs a perfect legal substantiation of the issue of organizing an effective fight against cyberterrorism in the context of intensifying global influences, new information technologies. The set of relevant legal acts should be constantly improved taking into account the relevant international legislation, its evolution and domestic legislative practice, which should be in the interests of national information activities.

The issue of legal regulation as the implementation of state functions, in particular to ensure cybersecurity and counter cyber threats should be based primarily on the general security of society, especially with regard to legal norms prohibiting certain actions - in particular, in relation to pre-destructive technologies. The main problem is the non-obviousness of destructiveness and possible errors in assessing the essence of technology, so the search for possible solutions to this series of problems is

promising for further research in the field of legal science.

In addition, state regulation of relations regarding the use of emerging technologies should be limited to the implementation of the economic function of the state, which is to ensure economic diversity as defined in Art. 15 of the Constitution of Ukraine. It should be about promoting a free market and state influence to prevent the abuse of monopolies and restrict economic competition. At the same time, the provision of various priorities and preferences must be justified and follow from the real need.

References

Almenar, F. (2020). Computer crime. Revista general de derecho procesal, 50, 202-212. Retrieved from https://cutt.ly/qxHBb1o

Azarov, D. (2007). Crimes in the field of computer information (criminal law research). Kyiv: Atika. Retrieved from https://law.ukma.edu.ua/azarov-d-s-zlochyny-u-sferi-komp-yuternoyi-informatsiyi-kryminalno-pravove-doslidzhennya/

Baturin, Yu. (1991). Problems of computer law, Moscow: Legal literature. Retrieved from http://lawlibrary.ru/izdanie7669.html

Bilenchuk, P. & Obihod, T. (2018). Cyber security and means to prevent and combat cyber crime and cyberterrorism. Journal of the Kyiv law university, 3, 235-239.

Brants, C., Johnson, D. & Wilson, T. (2020). New Wine in Old Bottles: Alternative Narratives of Cybercrime and Criminal Justice? Journal of criminal law, 84(5), 403-406.

Butuzov, V. (2010). Counteraction to computer crime in Ukraine (system-structural analysis). Kyiv: KIT. Retrieved from http://194.44.142.55/F?func=find-b&request=000267407&find_code=SYS

Council of Europe. (2001). European Convention on Cybercrime. Retrieved from https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

Djerf-Pierre, M. (2018). Squaring the Circle: Public Service and Commercial News on Swedish Television. Journalism Studies, 1(2), 239 – 260.

Dovgan, O. (2018). Cybersecurity in the information society: Information-analytical digest, Kyiv: Publishing house "Artek". Retrieved from http://nbuviap.gov.ua/images/vydannya/2018/bezpeka_no_1.pdf

Dovhan, O. and Tkachuk, T.U (2018). System of information security of Ukraine: ontological dimensions. Information and law, 1 (24), 89-103.

Europol. (2016). Public Awareness and Prevention Guides. Retrieved from https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cyber-crime-vs-cyber-security-what-will-you-choose

Gritsyak, N. (2015). Information component of state policy and management, Kyiv: K.I.S. Retrieved from http://academy.gov.ua/NMKD/library_nadu/Monogr/e008ca03-7c8b-49fa-9a91-1769523a94c7.pdf

Hong, Ye & Neilson, W. (2020). Cybercrime and Punishment. Journal of legal studies, 49(2), 431-466.

Moiseev, N. (2016). Information Society as a Stage of Contemporary History. Free Thought, 1, 81-83.

Nekit, K. (2020). Social media account as an object of virtual property. Masaryk University Journal of Law and Technology, 14 (2), 201-226.

Nekit, K. Ulianova, H. & Kolodin, D. (2019). Website as an object of legal protection by Ukrainian legislation. Amazonia Investiga, 8 (21), 222-230. https://amazoniainvestiga.info/index.php/amazonia/article/view/97

Oxford Advanced American Dictionary. (2021). Cyber-. Retrieved from https://www.oxfordlearnersdictionaries.com/definition/american_english/cyber

Pogoretsky, M. (2012). Cybercrime: to define the concept. Bulletin of the Prosecutor's Office, 8, 89–96. Retrieved from http://91.217.179.134:9100/libr/DocDescription?doc_id=1888355

Pozhuyev, V. (2016). Formation of the state information policy in the conditions of globalization. Humanitarian bulletin of the Zaporozhye State Engineering Academy, 43, 4–12. Retrieved from https://cutt.ly/AxH39UA

Rogovets, V. (2015). Information wars in the modern world: causes, mechanisms, consequences. Personal, 5, 10-17.Retrieved from https://cutt.ly/uxH8b6L

Statista. (2018).The level of Internet penetration in the world as of September 2018, broken down by region. Retrieved from https://www.statista.com/statistics/269329/penetration-rate-of-the-internetby-region/

Stets, V. (2019). Theoretical and legal problems of defining the essence of cyber security as a component of information security. Actual problems of public administration, 4(80), 24-28.

DOI: https://doi.org/10.35432/1993-8330appa4802019194098
Tamarit, J.M. (2020). Ciberdelincuencia: cómo facilitar la denuncia y el apoyo a las víctimas. Revista general de derecho penal, 34, 423-433.
Tench, R. & Yeomans, L. (2014). Exploring Public Relations. US: Pearson Education.
United Nation. (2000). Tenth UN Congress on the Prevention of Crime and Treatment of Offenders "Crime and Justice: Meeting the Challenges of the Twenty-first Century". Retrieved from https://www.unodc.org/congress/en/previous/previous-10.html
Yar, M. (2015). The Novelty of 'Cyber crime': An Assessment in Light of Routine Activity. Theory European Journal of Criminology, 2 (4), 407–427.