Кримінальне право та кримінологія; кримінально-виконавче право

УДК 343.3/.7:004.056.5(477)
DOI 10.33244/2617-4154.1(18).2025.182-188

H. V. Didkivska,
Doctor of Law, Professor,
Professor of the Department of Criminal Law and
Process of the State University of Kyiv
e-mail: galynadid@gmail.com
ORCID ID 0000-0003-1714-4804;
R. I. Elshad,
Ukrayna Azərbaycanlıları Radası
Director, PhD
e-mail: galynadid@gmail.com
ORCID ID 0000-0001-7296-5408

TOPICAL ISSUES OF COUNTERACTING CYBERCRIME IN UKRAINE

The beginning of the twenty-first century was characterized by the active development of computer technology. Computer technology plays an important role both in the everyday life of each of us and in the activities of the whole state. It is noted that rapid computerization has led to the emergence of new social relations – relations on the Internet (cyberspace). Cyberspace, in turn, has, in addition to the positive, a number of negative, criminal law characteristics, such as copyright infringement, spread of computer viruses, interference with the operation of information carriers, illegal use of information, and many other traditional and other types of criminal offenses which have been called cybercrime. The author emphasizes that cybercrime is a major problem of our time. The article examines the issues of cybercrime which have developed significantly and have caused serious concern among law enforcement and human rights agencies of many countries.

The article examines the issues of systematic growth of the number of information crimes and the dynamics of their spread. In addition, the systematic spread of virus programs, facts of unauthorized access to cyberspace information resources, and the unlawful theft of important information from databases which are not in the public domain are causing more and more negative consequences and pose a danger to society.

It is noted that one of the threats to national security in the information sphere, according to Article 7 of the Law of Ukraine "On the Fundamentals of National Security of Ukraine", is *computer crime and computer terrorism, and the Constitution of Ukraine calls ensuring information security the business of the entire Ukrainian people. In recent years, domestic law enforcement agencies have significantly strengthened their efforts to combat cybercrime. A separate Department for Combating Cybercrime within the structure of the Ministry of Internal Affairs of Ukraine, the Department for Counterintelligence Protection of the State's Interests in the Field of Information Security of the Security Service of Ukraine, and information security structures within ministries and other executive authorities have been established.*

Keywords: *cybercrime, criminal offense, national security, cyberspace, law enforcement agencies, cyberpolice, information sphere, counteraction, prevention.*

Research on the topic. A significant part of scientific works on cybercrime is devoted to O. M. Bandurko, V. V. Vasylevich, V. V. Golina, B. M. Golovkin, A. P. Zakaliuk, O. M. Lytvynov, V. V. Markov, M. I. Sashchenko, V. I. Trapeznikov, V. O. Tulyakov, I. V. Zhuk, Ya. V. Levkivska and others. However, the problem of modern mechanisms for combating cybercrime is one that constantly requires scientific analysis and study.

Purpose of the study. To analyze cybercrime in the modern world as the most dynamic type of criminal offense, which is a rapid trend in development, which is due to the constant development of computer technologies. Define cybercrime as a type of crime whose participants use electronic computing machines (computers), automated systems or telecommunications networks, other modern technical developments (devices), and artificial intelligence programs to achieve a criminal result.

Relevance. Modern research on cybercrime indicates the need to improve mechanisms for combating cybercrime in Ukraine and actively promote the implementation of innovations, primarily at the state level. It would be appropriate, first of all, to improve the categorical apparatus, to provide at the legislative level the possibility of conducting independent inspections of entities providing digital services to the population, to provide police units with new functions to combat cybercrime by issuing a relevant regulatory act, to promote the establishment of close cooperation with EU institutions, joint activities of the public and research centers with state institutions to combat cybercrime, based on EU standards.

Main presentation of the material. Today, computer crimes are the most dynamic group of socially dangerous offenses. The speed of spread of these offenses directly depends on the development of technologies and technical programming of the population, as well as the constant improvement of computer technology. In the scientific community, it is noted that cybercrime, cyberfraud and theft of information data have become an effect of the regression of social development in the field of computerization. For example, in 2000, no cases of using a computer to commit a criminal offense, in particular, stealing someone else's personal data or seizing bank accounts, were detected, but already in 2001, according to the Ministry of Internal Affairs, 5 such crimes were registered, in 2002 the number increased to 30, in 2007 – 146, and in 2020 their number significantly increased to 108,474, which was most likely due to quarantine measures against COVID-19 [1].

Currently, there is a characteristic increase in political and economic tension in cyberspace, in the territory of which hybrid information warfare is taking place. One of the common methods of conducting cyberattacks is the well-known DDoS attacks. Most often, such attacks fall on state institutions and web-resources of news, which in one way or another cover events in individual countries and the world as a whole. The most popular DDoS attacks today and possible trends in their development in the future. The first thing that distinguishes DDoS attacks of 2013 and 2014 from previous ones is the use of several vulnerability vectors. As is known, one vector is enough to hit the target and cause guaranteed damage, which increases the probability of success of a multi-vector attack. In addition, such tactics confuse the IT staff of the attacked organization. Considering DDoS attacks in general, in 2014 attacks aimed at web resources continued to dominate as the fastest vector. Since 2013, there has been a clear increase in DDoS attacks on software applications as a result of the presence of systems for protecting organizations against network DDoS attacks deployed in recent years. In addition, network attacks are much easier to counteract and do not belong to the category of attacks that are difficult to prevent [2].

Today, most attack defenses are sufficiently developed that organizations can counter DDoS attacks targeting networks and software applications for quite a long time without damaging the IT infrastructure. But attackers can use many attack vectors in search of those weak points that are not provided for by the DDoS defense solution in the field of countering cybercrime. More than half of the cases are DDoS attacks with five or more vectors. Often, attackers do not plan to use the entire spectrum of the provided arsenal, giving the “victim” the opportunity to process the attack vector sequentially. In the case of blocking one attack vector, the attackers will use the next one. This leads to the fact that during a massive DDoS attack there will be at least one vector that cannot be repelled and will reach the final goal. In most cases, the result of a DDoS attack is a down or slow web server, but recently DDoS attacks are not only aimed at web servers. The main targets of modern DDoS attacks are increasingly becoming the Internet channel and the firewall. Another feature of modern DDoS attacks is a significant reduction in the cycles of implementing new methods to bypass the protection system [3].

A significant reason that leads to such a result is HTTP flood-type cyberattacks. They begin when the attacker sends a large number of HTTP GET / POST requests, undermining server resources. At the same time, although HTTP attacks remain the most common, SSL-encrypted attacks remain dangerous because they are difficult to counteract. Fraud, hacking activity, as well as a long list of privacy requirements have led organizations to use the HTTPS protocol and encrypt communications automatically. According to market research reports, more than 90 % of organizations use HTTPS for any publicly available interaction with the WEB. HTTPS messages are usually decrypted at a very late stage of the organization’s internal network. Attackers use this feature of encrypted messages as a means of bypassing security solutions (anti-DoS/DoS, firewalls and IPS / IDS), which ultimately fail to detect the attack. An additional interesting feature of SSL-based DoS / DoS attacks is the asymmetric nature of SSL encryption, the peculiarity of which is that decrypting messages takes almost ten times more resources than encrypting them. Using this asymmetric feature, criminals can create a devastating attack with relatively low resources. Using methods to bypass protection systems, attackers manage to deliver malicious messages deep into the network, where servers and various modules are more vulnerable to high traffic volumes to observe suspicious delays or complete shutdowns. SSL-encrypted attacks are a new trend that will increase over the years and according to experts, more than half of DoS attacks will be SSL-encrypted. Thus, DDoS attacks are and will be in the coming years the most popular means of causing economic losses from downtime of online services, as well as for undermining the reputation of political and media organizations by refusing to service official websites. Such attacks have received a special increment of development with the increase of political and economic confrontation in the world, which makes them more unpredictable. All the above factors force relevant organizations to consider the issue of development and development of systems for countering such cyberattacks [3].

So, cybercrime is currently understood as a type of criminal offense committed in the Internet space (cyberspace) using mathematical, digital or symbolic techniques that are in constant dynamics. Unlike other groups of crimes that have been developing for several centuries: theft, fraud, murder, computer crimes are a relatively young socially dangerous phenomenon that began its existence with the advent of the Internet. Such features as scale; anonymity, speed of information transfer; global audience, a large number of services that are interconnected, make the Internet favorable for committing criminal acts, since detecting such actions is a more difficult task for the law enforcement system. Responsibility for this type of illegal actions is provided for by Chapter XVI of the Criminal Code of Ukraine. The historical development of cybercrime begins in the 60s of the 20th century and includes the following stages: – the emergence of the first Internet servers; – the emergence of the first Internet viruses; – first application of liability to a cybercriminal, USA 1983 – adoption of the first regulatory legal act prohibiting the spread of Internet viruses, USA 1986 – adoption of the Council of Europe Convention on Cybercrime, 2001 The issue of the theoretical definition of cybercrime lies in the forensic study of this phenomenon. Thus, the object of cybercrime is the sphere of social relations that exists within the information field. That is, such relations that arise in the process of using electronic computer networks, automated systems and telecommunication networks. The subject of a criminal offense is a general person – a sane person who has reached the age of criminal responsibility.

It is worth noting that some criminal offenses in criminal law require the presence of a special subject.

The method of committing cybercrimes may vary depending on the means of committing a criminal offense. Thus, the methods may be: direct access to information contained on information carriers and methods of remote access to the same information. Therefore, it is possible to distinguish the main features of cybercrime as a socially dangerous phenomenon: − the sphere of commission of such offenses is cyberspace; − this group of offenses includes a number of relations related to the use of electronic computer networks, automated systems and telecommunication networks; − in their majority, cybercrimes involve the presence of direct intent on the part of the offender; − the means of their commission are computer systems, automated systems and telecommunication networks. No less important is the definition of the classification of information crime, since it should be useful in studying the essence of a socially dangerous act. Understanding the types of cybercrimes is important for building a mechanism for detecting, investigating and counteracting crimes in the field of computerization. Analyzing the regulatory framework and scientific achievements on the classification of cybercrimes, it is worth noting that the most appropriate division is contained in the Council of Europe Convention on Cybercrime. It is based on the generic object of the type of offense under study and is the basis for building the legislation of developed countries. In scientific circles, there are many views on the division of cybercrimes, the most famous of which is the division according to the generic object: − offenses for which liability arises on the basis of Section XVI of the Criminal Code of Ukraine; − offenses for which liability is provided for by various Sections of the Criminal Code of Ukraine. The Criminal Code of Ukraine does not contain a clear division of offenses in the field of computerization. We can agree that this is not a positive aspect, since difficulties arise in the process of qualifying the actions of persons who committed the offense. Thus, in most cases, liability arises for criminal offenses provided for in Article 361 of the Criminal Code of Ukraine, and the least applied, to date, is Article 363 of the Criminal Code of Ukraine. Another problem is the application by courts of milder punishments for individuals than provided for in the article of the Criminal Code of Ukraine, as well as the failure to apply additional types of punishments in the form of confiscation of property, especially for things with which a criminal offense was committed. Statistics have shown that the level of convictions in relation to the level of offenses committed is very low. Currently, there is a need for the modern legal system of Ukraine to be modernized in accordance with European standards, namely in the field of detecting, investigating and combating cybercrime. A modernized legal system would help to avoid problems in the field of understanding the internal structure, the phenomenon under study, the qualification of the actions of persons who committed offenses and the imposition of punishment for them. Today, the issue of ensuring cybersecurity is becoming relevant, which is the level of protection of the interests of a person and a citizen, society and the state when using cyberspace, as well as the ability to identify, prevent and neutralize real and potential cybersecurity threats. The fundamental principles on which the current legislation of Ukraine in the field of countering cybercrime is based are general and international principles: the rule of law, legality, ensuring the national interests of the state, proportionality and adequacy of cybersecurity measures to real and potential risks, the priority of preventive measures, mutual assistance regarding the rules on mutual assistance, and others. The organizational foundations of the investigation of information and computer crimes in Ukraine today are investigative actions at the initial and subsequent stages of the investigation. Therefore, in order to prevent the spread of crimes in cyberspace (legal regulation is provided for by the relevant articles of the Criminal Code of Ukraine), operational and investigative groups must, firstly, carry out a complete collection of the necessary information from the local device or computer of the criminal, and secondly, organize the detention of the criminal, interrogate witnesses, suspects and, if any, accomplices in the commission of a specific cybercrime [1].

As we can see, our state is faced with a number of pressing issues that affect the reduction of the effectiveness of countering cybercrime, the level of which is only increasing every year.

Studying the analysis of world experience in combating cybercrime, one can note the undeniable role of the USA, the EU and Canada in the development of this area. It is necessary to note the huge contribution of the USA, which created the Cyber Police Department in the state of New York, the main functions of which are the implementation and development of a long-term national policy to protect the state from attacks by cybercriminals, and the Safe Childhood project, which ensures the prevention of sexual exploitation of children on the Internet. The experience of the European Union is also positive, which is distinguished by the creation of a single unified system of Operational Security Centers operating throughout the Union of democratic European countries, and the introduction of a system of so-called "cyber sanctions". Success in implementing national policy in the field of combating cybercrime was achieved by Canada, which contributed to the creation of a stable system of municipal police units, which were assigned additional functions by law in the fight against cybercrime [1].

Conclusion. It is seen that one of the main tasks that needs to be solved is to improve and unify in the current regulatory legal acts of Ukraine a clear definition of concepts in the field of cybercrime; to provide special security mechanisms designed to control cyberspace and the phenomena occurring in it; to strengthen the human resources potential of the state's law enforcement agencies to combat cybercrime, and other countermeasures.

LIST OF SOURCES USED

1. URL : https://isg-konf.com/wp-content/uploads/2022/04/Monograph/Doi/Legal/ISG.2022.MONO.LEGAL.1.2.3.pdf

2. Ledovsky V. Modern DDoS attacks and protection against them using Radware Attack Mitigation System / Analytical center Anti-Malware. URL : http://www.antimalware/analytics/DDoS_protection_Radware_Attack_Mitigation_System – 27.03.2013.

3. Quarterly Global DDOS Attack Report: Q2 2013 / Akamai. URL : http://www.prolexic.com/knowledge-center-ddos-attack-report-2013-q2.html – July 17, 2013.

Г. В. Дідківська, R. I. Elshad. АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Початок двадцять першого століття охарактеризувався активним розвитком комп'ютерних технологій. Комп'ютерна техніка відіграє важливу роль як у повсякденному житті кожного з нас, так і в діяльності цілої держави. Зазначається, що швидка комп'ютеризація потягнула за собою виникнення нових суспільних відносин – відносин в інтернеті (кіберпросторі). Кіберпростір зі свого боку має, крім позитиву, ряд негативних, кримінально-правових характеристик, таких як порушення авторських прав, розповсюдження комп'ютерних вірусів, втручання в роботу інформаційних носіїв, незаконне використання інформації, та багато інших, як традиційних, так і інших видів кримінальних *правопорушень, які були названі кіберзлочинами. Акцентується увага на тому, що кіберзлочиність є великою проблемою сучасності. Досліджуються питання кіберзлочинності, які набули суттєвого розвитку, що спричинило серйозне занепокоєння в системи правоохоронних та правозахисних органів багатьох держав.*

У статті досліджуються питання систематичного зростання кількості інформаційних злочинів та динаміка їх поширення. Також систематичне розповсюдження програм-вірусів, фактів несанкціонованого доступу до інформаційних ресурсів кіберпростору, протиправне викрадення важливої інформації з баз даних, що не перебуває в загальному доступі, спричиняє дедалі більше негативних наслідків та несе небезпеку для суспільства.

Зазначається, що однією із загроз національній безпеці в інформаційній сфері згідно зі ст. 7 Закону України «Про основи національної безпеки України» визначено комп'ютерну злочинність і комп'ютерний тероризм, а в Конституції України забезпечення інформаційної безпеки названо справою усього українського народу. За останні роки вітчизняні правоохоронні органи значно підсилили напрям протидії кіберзлочинності. Було створено окреме Управління боротьби з кіберзлочинністю у структурі Міністерства внутрішніх справ України, Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України, структури із захисту інформації у складі міністерств та інших органів виконавчої влади.

Ключові слова: *кіберзлочинність, кримінальне правопорушення, національна безпека, кіберпростір, правоохоронні органи, кіберполіція, інформаційна сфера, протидія, запобігання.*

Стаття надійшла до редколегії 28 січня 2025 року