UDC 343.13
DOI https://doi.org/10.32782/pyuv.v3.2024.38

Ya. P. Kharchenko
orcid.org/0009-0004-9997-7088
Postgraduate at the Department of Criminal Justice
State Tax University

CRIMINAL LAW COUNTERACTION TO CRIMINAL OFFENSES IN THE FIELD OF EXPLOITATION OF ELECTRONIC COMPUTING EQUIPMENT

Actuality of theme. According to periodic reports of the leadership of the Cyber Police Department of Ukraine, the number of criminal offenses in the field of computer technology use is increasing every year. And accordingly, such a situation requires qualified personnel both in the field of detection of criminal offenses in the field of exploitation of computer equipment, which are extremely intellectual crimes, and in the field of protection of the interests of victims. The main types of computer crimes specified in the Convention on Cybercrime, which Ukraine ratified in 2005, are constantly being modified, improved and supplemented with new types. Currently, we can talk about the following types of such offenses: illegal access to computer systems by criminals; illegal interception of computer information without the right to such interception; Targeted interventions in computer systems with the subsequent destruction, damage, deterioration or alteration or concealment of information without appropriate permission.

So, as we can see, today the world has undergone radical reforms. Yes, currently, we cannot imagine our life without the Internet, computers, smartphones and other modern technologies. Along with the real world, the virtual world is developing, which in the future may affect the spheres of our everyday life. This development is a consequence of the so-called digital revolution, which is taking place thanks to the development of IT technologies. Progress does not leave anyone behind, which led to the appearance of such a phenomenon as cybercrime. All over the world, criminal offenses in the field of exploitation of electronic computing equipment, or cybercrime, in cyberspace from year to year cause losses of tens of billions of US dollars both to individuals and private companies and to states as a whole.

Analysis of recent research and publications. In modern criminology, more and more topics are raised for discussion of the problem of cybercrime as a threat to the information space and are in the field of interests of an increasing number of scientists and practitioners. Among the cohort of well-known scientists O. M. Bodunova, M. V. Gutsalyuk, G. V. Didkivska, M. O. Kravtsova, V. V. Markov, Yu. V. Nikitin, E. D. Skulysh, V. V. Topchii, others. Despite this, there is still a need for further research into the criminological protection of cyberspace from criminal offenses in the field of exploitation of electronic computing equipment, which, in our opinion, will allow us to provide a certain understanding of the danger of cybercrime for society.

Presenting main material. Criminal offenses in the field of exploitation of electronic computing equipment are defined as cybercrimes and are defined in the professional literature as "criminal offenses committed in cyberspace with the help of special devices (computers, smartphones, tablets, terminals and others), automated systems, computer networks or telecommunication networks, and related to illegal, unauthorized creation, storage, processing, forgery, blocking, destruction of information infrastructure objects» [1].

In accordance with the above, cybercrime can be considered to encompass various spheres of life in society, and anyone can become a victim of such an offense.

So why does this type of criminal offense spread so quickly to all areas of our life. The answer, as you can see, is very simple, a large percentage of the fact that the act will remain unnoticed by law enforcement agencies. Criminal offenses in the field of exploitation of electronic computing equipment are quite latent.

In the conditions of war, in which Ukraine is located, such criminal offenses can be committed with the aim of destabilizing the situation in unoccupied territories, theft of confidential information, sabotage of state-owned enterprises, tasks of other grave consequences.

The latency of criminal offenses in the field of exploitation of electronic computing equipment/ cybercrime in professional literature is explained by the following features: "committing such a criminal offense requires a certain set of knowledge; cybercrimes, unlike other intellectual crimes, are accessible to people of low social and age capabilities; to commit cybercrimes, one does not need to occupy a high social position, it is enough to have access to the Internet and electronic computing equipment; anonymity and impersonality of cybercrimes – cyberspace identification mechanisms allow a person to use anonymously or impersonate another person, change biographical data or social status.

In wartime, such a cybercriminal becomes a combat unit, and his main activity is cyberattacks and hacking. In addition, during martial law, attacks are possible both from the side of the enemy, who uses the information space to damage Ukraine's defense capabilities, and from those who have decided to take advantage of the situation, the overload of law enforcement agencies, for their own enrichment. So, nowadays, a war in the information space can cause no less damage than a war on the battlefield. Understanding this, in the first month of the war, the parliament quickly optimized criminal and criminal procedural legislation, improving the grounds and procedural mechanisms for bringing cybercriminals to criminal responsibility [2].

Currently, there is a trend of increasing cyberattacks in Ukraine, therefore, in the conditions of war, there is a need to strengthen criminal responsibility.

On February 1, 2022, the President by decree No. 37/2022 put into effect the decision of the National Security Council "On the Plan for the Implementation of the Cybersecurity Strategy of Ukraine" – law enforcement agencies must minimize cybercrime.

The Criminal Code was not coordinated with the legislation in the field of cyber security and did not ensure the completeness and comprehensiveness of the investigation of cybercrimes, and the responsibility was disproportionate to the damage to the state and society.

That is why parliamentarians have optimized to counter cyber threats: 1. Art. 361 of the Criminal Code of Ukraine – cyber attack; 2. Art. 361-1 of the Criminal Code of Ukraine – creation, distribution and sale of malicious programs or techniques for cyber attacks. The Law of Ukraine "On Amendments to the Criminal Code of Ukraine on Improving the Effectiveness of Combating Cybercrime in the Conditions of Martial Law», entered into force on 04/03/2022 (Published in the Voice of Ukraine on 03/02/2022), according to which: – Art. 361 and 361-1 of the Criminal Code of Ukraine are harmonized with the legislation in the field of cyber security; – in Art. 361 of the Criminal Code of Ukraine demarcated the severity of the punishment for a cyberattack depending on the consequences and increased the punishment – from a fine to 15 years in prison; – search and detection of vulnerabilities is not a cyber attack (Part 6 of Article 361 of the Criminal Code of Ukraine); – increased punishment under Art. 361-1 of the Criminal Code of Ukraine – from a fine to 5 years in prison [3].

But at the moment, the criminal legislation does not specify other types of criminal offenses that are also classified as cybercrimes.

Such criminal offenses may include: computer-related forgery, intentional alteration, destruction or concealment of data that creates new invalid data; this is fraud related to computer technology, which usually leads to the loss of property of any person; offenses related to the production and distribution of child pornography; criminal offenses in the field of infringement of copyright or related rights and related criminal offenses.

But, nevertheless, the legislation of Ukraine establishes criminal responsibility for crimes in the field of using computers, systems and computer networks and telecommunication networks. The Criminal Code of Ukraine provides for the maximum punishment of up to six years of imprisonment for the above-mentioned crimes.

Also, in accordance with the Law of Ukraine "On Electronic Communications" and the requirements of other legislation of Ukraine in the field of cyber security, the term "electronic computing machines (computers), automated systems, computer networks or telecommunication networks" was replaced by "information (automated), electronic communication, information and communication systems, electronic communication networks".

The current state of affairs requires every modern socially active person in Ukraine to use mobile devices and use the Internet, state bodies conduct electronic document management, "the stable operation of financial institutions, railways and air transport, large enterprises also depends on the stability of the cyberspace with which they are forced to work, and communication is provided using electronic means of communication".

Studying the history of the development of crime, it is worth paying attention to one regularity, where new social relations develop, crime also appears there. According to the official statistics of the Office of the Prosecutor General of Ukraine, for the last time the number of detected criminal offenses in the field of exploitation of electronic computing equipment increased by almost 7.5 times (and this does not take into account classic offenses involving the use of computer equipment, as well as the level of latency of such crime).

It is worth mentioning the failed attack attempt by the hacker group Strontium, who tried to gain access to computer networks in Ukraine, the USA and the EU in order to provide tactical support for Russia's physical invasion of Ukraine and steal confidential information.

At the beginning of the full-scale invasion of the Russian Federation, the State Intelligence Service reported that Ukrainian users had received new dangerous e-mails with the subject "No. 1275 dated 04.07.2022", the opening of which leads to hackers

gaining full control over your computer and threatens to steal and damage computer information.

Earlier, the State Intelligence Service warned about the distribution of e-mails with the name "Military criminals of the Russian Federation. htm", the activation of which leads to the fact that hackers get remote access to anyone's computer.

Critical infrastructure facilities are also targeted. The Ukrainian provider Ukrtelecom suffered a powerful attack on March 28, 2022, during which hackers tried to analyze how the IT infrastructure is arranged, disable equipment and services, as well as gain control over the network and equipment of companies of all forms of ownership.

On March 23, of the same year, the enemy tried to carry out a cyber attack on the state institutions of Ukraine using the malicious program Cobalt Strike Beacon, which destabilizes the operation of the computer in the event of its opening. These are examples of massive attacks only. Smaller attacks and individual cases of personal hacking are simply not reported.

Taking into account the constant development of modern technologies, there is a need for constant updating of cyber protection in the sphere of cyberspace. The open invasion of the Russian Federation accelerated the improvement of current legislation and security guarantees in the modern information IT space.

Currently, during a war, state bodies, large enterprises, defense and critical infrastructure enterprises, as well as enterprises that provide the population and defense with everything necessary in war conditions are at risk. There are also risks for local residents who are in the war zone. During martial law, everyone should pay attention to several aspects of control: for companies, authorities and officials, the presence of a technical specialist from a specialized company will significantly increase the level of cyber protection. Professionals are able to complicate the work of the enemy by introducing the necessary protection algorithms, including organizational ones, in the company.

There is a need to train employees who perform work related to the relevant systems and networks, because many attacks achieve the goal of hacking due to ill-considered and careless actions of employees themselves.

Next, those who are in the cyber risk zone should be given recommendations on following up on relevant messages on the official resources of the State Special Communications and CERT-UA. Such resources publish official warnings to obtain information about possible cyberthreats, and about what opportunities there are to minimize certain risks.

In the event of a cyber attack, it is suggested to immediately notify those to whom such an attack may spread. For individuals, these are the contacts of those with whom active communication is carried out. For companies and authorities, there can be employees, customers, counterparties and business partners. It is also important to inform the official subjects of the cyber security of Ukraine, CERT-UA and the Cyber Police. This will provide an opportunity to take operational measures and block harmful web resources.

First of all, the defender himself must have an idea of the structure of the computer network, know the means of recording illegal interference, methods of identifying criminals.

Therefore, when developing modern mechanisms to prevent such crime, other derivative circumstances should be taken into account. For example, the somewhat low level of qualification of judges on issues of criminal offenses in the field of operation of electronic computing equipment.

Also, there are criminal offenses that are committed with the help of Internet resources, for example, the sale of illegal drugs and weapons. There are cases when in Ukraine, people who create virtual casinos on the Internet or create pseudo trading platforms on the so-called Forex resource receive sentences.

Legal support of such criminal proceedings currently requires sufficient knowledge of the field of IT technologies, [5] or at least certain ideas about how virtual space works.

Conclusion. As we can see, there is a basis for the legislative provision of mechanisms for effective cyber protection in the conditions of martial law. And it has existed since the beginning of the 2000s, when Ukraine ratified the international convention on the prevention of cybercrime dated November 23, 2001. Currently, everyone's task, when a cyber attack is detected, remains to activate this mechanism as soon as possible, so that in the future similar cyber attacks and interventions and losses from them become less and less. And repelling such attacks became more and more effective. In our opinion, for this it is necessary to constantly improve legal support in the field of protection against cybercrime.

References

1. Кривенко К. Кіберзлочинність: актуальна судова практика. *Liga Zakon* : веб-сайт. URL: https://biz.ligazakon.net/analitycs/209283_kberzlochinnst-aktualna-sudova-praktika (дата звернення: 29.07.2024).

2. Кримінальні відповідальність за кіберзлочини. *Довідково-інформаційна платформа правових консультацій "WikiLegalAid"* : веб-сайт. URL: https://wiki.legalaid.gov.ua/index.php/%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%B2%D1%96%D0%B4%D0%BF%D0%BE%D0%B2%D1%96%D0%B4%D0%B0%D0%BB%D1%8C%D0%BD%D1%96%D1%81%D1%82%D1%8C_%D0%B7%D0%B0_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%

D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%B8 (дата звернення: 24.07.2024).

3. Посилено кримінальну відповідальність за кіберзлочини. *Юридична компанія «Капітал» :* веб-сайт. URL:https://capital-ukraine.com/posyleno-kryminalnu-vidpovidalnist-za-kiberzlochyny (дата звернення: 29.07.2024).

4. Єрема М., Борисенко А. Боротьба з кіберзлочинністю в умовах дії воєнного стану : Закон 2149-IX. *Liga Zakon* : веб-сайт. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix (дата звернення: 29.07.2024).

5. Чорна А. Принципи запобігання поліцією кримінальним правопорушенням на деокупованих територіях. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2023. № 2. URL: https://visnik.dduvs.in.ua/wp-content/uploads/2023/08/2/NV_2-2023-43-47.pdf (дата звернення: 29.07.2024).

Анотація

Харченко Я. П. **Кримінально-правова протидія кримінальним правопорушенням у сфері експлуатації електронно-обчислювальної техніки.** – Стаття.

У даній статті зазначається, що кіберзлочини, це нові та високотехнологічні кримінальні правопорушення, які потребують суттєвого удосконалення кримінального законодавства та кваліфікованих кадрів для захисту потерпілих від таких кримінальних правопорушень, та злочинців що їх вчинили. Перш за все, тим хто протистоїть кіберзлочинності самим потрібно мати уявлення про структуру комп'ютерної мережі, знати засоби фіксації протиправного втручання, методи ідентифікації злочинців.

Зазначено, що при розробці сучасних механізмів запобігання такій злочинності, слід враховувати дещо низький рівень кваліфікації суддів з питань кримінальних правопорушень у сфері експлуатації електронно-обчислювальної техніки .

Вказується, що існують кримінальні правопорушення, які вчиняються за допомогою інтернет ресурсів, наприклад, продаж заборонених у вільному обігу наркотичних засобів, зброї. Є випадки коли в Україні, отримують вироки особи, що створюють в мережі інтернет віртуальні казино, чи створюють псевдо трейдерські платформи на так званому ресурсі Forex.

Юридичний супровід таких кримінальних проваджень також потребує достатніх знань сфери IT технологій, або хоча б певні уявлення про те як працює віртуальний простір.

Зазначено, що підґрунтя законодавчого забезпечення механізмів для ефективного кіберзахисту в умовах воєнного стану існує. І існує воно ще з початку двохтисячних років, коли Україна ратифікувала міжнародну конвенцію із запобігання кіберзлочинності від 23 листопада 2001 року. Акцентується увага на тому, що завданням кожного, при виявленні кібератаки залишається як найшвидше активувати цей механізм, щоб у майбутньому подібних кібер нападів та втручань і збитків від них ставало дедалі менше. А відсіч таких атак ставала все більш ефективнішою.

Ключові слова: запобігання, злочинність, кібератаки, кримінальні правопорушення, кримінально-правова протидія, кримінологія, електронно-обчислювальна техніка, кіберзлочин, кримінально-правове забезпечення.

Summary

Kharchenko Ya. P. **Criminal law counteraction to criminal offenses in the field of exploitation of electronic computing equipment.** – Article.

This article states that cybercrimes are new and high-tech criminal offenses that require significant improvement of criminal legislation and qualified personnel to protect victims of such criminal offenses and criminals who committed them. First of all, those who oppose cybercrime themselves need to have an idea of the structure of the computer network, know the means of recording illegal interference, methods of identifying criminals.

It is noted that when developing modern mechanisms to prevent such crime, one should take into account the somewhat low level of qualification of judges in matters of criminal offenses in the field of exploitation of electronic computing equipment.

It is indicated that there are criminal offenses that are committed with the help of Internet resources, for example, the sale of illegal drugs and weapons. There are cases when in Ukraine, people who create virtual casinos on the Internet or create pseudo trading platforms on the so-called Forex resource receive sentences.

Legal support of such criminal proceedings also requires sufficient knowledge of the field of IT technologies, or at least some idea of how virtual space works.

It is noted that the basis for the legislative provision of mechanisms for effective cyber protection in the conditions of martial law exists. And it has existed since the beginning of the 2000s, when Ukraine ratified the international convention on the prevention of cybercrime dated November 23, 2001. Attention is focused on the fact that the task of everyone, when a cyber attack is detected, remains to activate this mechanism as soon as possible, so that in the future such cyber attacks and interventions and losses from them become less and less. And repelling such attacks became more and more effective.

Key words: prevention, crime, cyberattacks, criminal offenses, criminal law enforcement, criminology, computer technology, cybercrime, criminal law enforcement.