DOI: 10.18372/2307-9061.56.14904
УДК 342.7(045)

V. Filinovych,
Candidate of Law
ORCID ID: https://orcid.org/0000-0001-8824-615X

PROBLEMS OF HUMAN RIGHTS VIOLATIONS CAUSED BY CYBERCRIMES AND WAYS TO OVERCOME THEM

National Aviation University
Liubomyra Huzara Avenue, 1, 03680, Kyiv, Ukraine
E-mail: vvfilinovich@gmail.com

Purpose: *the purpose of the study is to critically evaluate cyber threats and their negative impact on the rights and freedoms of Ukrainian citizens.* ***The methodological basis*** *of the research comprises philosophical, ideological, general scientific and special methods.* ***Results:*** *most countries of the world are faced with problem of cybercrime. In Ukraine, the corresponding law on cybersecurity has already been enacted, and the country is trying to use its potential to protect the rights and freedoms of its citizens from abuse in the cyber environment. The author underlines that the issue of responsibility of state bodies and the state itself for violation of citizens' rights in the field of cybercrimes should be worked out in more detail at the legislative level.* ***Discussion:*** *improvement of the national legislation in the sphere of cybersecurity on the example of the normative acts of other countries; search for methods and actions to be taken while dealing with the consequences of cybercrimes.*

Keywords: *cybercrime; cybersecurity; cyberspace; violation of human rights; cyber environment; protection of citizens' rights in cyberspace; cyber attack.*

Problem statement and its relevance. Today cyber attackers significantly harm not only the national economy but also organizations and individuals. The rapid pace of the development of cybercrime is giving rise to more and more new trends in this area.

Therefore, the Ukrainian government is obliged to study and interact with new technologies, to understand the opportunities that these technologies provide to potential criminals. It is also important to understand how such technologies can be used as a tool to resist cybercrime.

Analysis of research and publications. The issue was studied by P. Sandle, J. Lewis, M. Rouse, D. Halder, K. Jaishankar and other scientists.

Purpose of the article. In this article the author wants to reveal the features of cybercrimes and critically evaluate its impact on citizen`s rights and freedoms.

The presentation of the main material. Today, concepts such as hacking, botnets, and cybercrime have become part of our daily speech, because cybercriminals use modern technology for their criminal purposes - to carry out cyberattacks against individuals, organizations, and even entire governments and states. Neither physical nor virtual boundaries are known to this type of illegal activity. However, they cause serious damage to the whole world.

In this regard, even traditional forms of crime have evolved, because dishonest organizations began to increasingly turn to the World Wide Web to facilitate their activities and maximize profits in a shorter time. These cybercrimes are not fundamentally new, but they are taking place in a new online dimension.

Before proceeding toward the analysis of methods of resisting violations of the rights of citizens in the cyber environment, one should form in his imagination some concepts and definitions that are inextricably linked with the research topic. These are,

of course, the concepts of cybersecurity, cyber environment, cybercrime, cybercriminal, and others.

There is still no single and stable concept of cybersecurity, nevertheless, according to the author of this study, the opinion of CISCO specialists, which is a recognized world leader in the field of high technologies, can be used as a definition. Yes, they are convinced that cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. At the same time, it is indicated that cyberattacks are usually aimed at accessing, modifying, or destroying confidential information; extortion of money from users; or interruption of normal business processes [3].

Cyberspace or digital environment is an interactive information space that operates using computer systems. If we turn to regulatory sources, then cyberspace should be understood as a virtual space, through the use of which it is possible to carry out communication and implementation of public relations. Such an environment was formed as a result of the functioning of interconnected communication systems and the provision of electronic communications using the Internet or other global data transmission networks [7].

Now let's take a closer look at "negative" cyber terms. For example, M. Rose of TechTarget notes that cybercrime is any criminal activity in which a computer, network (global, local) is involved. And although most cybercrimes are committed with the aim of making a profit by cybercriminals, a number of offenses are aimed against computers or gadgets directly with the aim of damaging or disabling them [2].

Thus, according to the US Department of Justice, cybercrime can be divided into the following three categories:

1) crimes in which the device is used as a weapon. An example of this is launching a (Distributed) Denial-of-service attack (DoS) through a computer;

2) offenses in which the computer is the target. An example of this is getting unauthorized access to the network;

3) crimes in which a computer is an accomplice in a wrongful act. An example is the use of such a technique for storing information obtained illegally [2].

According to I. Chekunov, there are 4 groups of cybercrimes:

1) those that are directly related to computers;

2) those related to the content of materials (content);

3) those that are against the confidentiality, integrity, and availability of computer data and systems;

4) those related to the infringement of copyright and related rights [11, p. 182].

D. Halder and K. Jaishankar are convinced that cybercrime should be viewed from a gender perspective. These experts talk about cybercrime against women, that is, crimes directed against women to deliberately inflict psychological and (or) physical harm on them, while using modern telecommunication networks and cell phones [1].

As for the personality of the cybercriminal, now we are talking about the whole criminal business and not individual self-taught hackers. As V.Yu. Rogozin says, at the moment we can observe the stratification of cyber intruders into:

1) persons who have significant knowledge in this specific area;

2) persons who have got their hands on a ready-made algorithm and at the same time have a very general understanding of the processes taking place in information systems.

The distinguishing features of the first group of criminals are their high professional and intellectual skills, the ability to commit crimes anonymously, in most cases cross-border. Also, usually, a large number of victims suffer from their actions, although the attackers did not come into direct contact with the victims [10, p. 58].

Considering all of the above, a logical question arises: who should be held responsible to citizens for violation of their rights in the field of cyberspace? Summing up the concept and characteristics of cybercrime, it becomes clear that it is, first of all, ordinary people, citizens of the country who suffer from it. Therefore, it is the state and its bodies that should be responsible for non-observance of the rights and freedoms of their citizens through the commission of cybercrimes against them.

If we talk about the responsibility of state bodies, then one can pay attention to both the failure to provide the relevant bodies for the protection of

human rights, and to the direct commission by such bodies of the relevant cyber-legal attackers.

In this context, Babajanyan K.A. writes about the legal responsibility of the state to an individual, which, in his opinion, can be expressed in both positive and negative forms. According to the scientist, the state, first of all, bears general positive responsibility for creating the necessary conditions for its citizens to exercise their rights and freedoms known as constitutional rights, as well as for maintaining proper public order in our country. The state should always be responsible for ensuring the personal safety of members of society, their protection from criminal attacks [4, p. 38]. Accordingly, the state must be held accountable for failing to provide a citizen with protection from criminal encroachment in the cyber environment.

We can also speak about the constitutional responsibility of the state over its citizens. So, according to Art. 55 of the Ukrainian Constitution, the court should protect human and civil rights and freedoms, and everybody has the guaranteed right to appeal in court against the actions or inaction of public bodies ... [6, Art. 55]. As indicated in Art. 2, 7 of the Law "On the Judicial System and the Status of Judges", the task of judges is to ensure everyone the right to a fair trial when administering justice on the rule of law bases. And the direct implementation of such a right envisages, inter alia, ensuring access to justice for every person, which, in turn, is ensured following the Constitution and under the procedure established by Ukrainian laws [9, Art. 2, 7].

Consequently, public officials and the state itself bear not only legal but other types of liability for failure to comply with and failure to provide proper assurance for the rights and liberties of their inhabitants who have suffered from acts of cybercrime.

It is important to note that in 2018, on May 9, Law of Ukraine 2163-VIII “On the Basic Principles of Ensuring Cybersecurity of Ukraine” (hereinafter referred to as the Law) has already come into force, due to which the level of juridical literacy of our residents in this sphere has significantly increased.

The corresponding normative legal act indicates the juridical and organizational base for guaranteeing the protection of the national interests of our country in cyberspace, as well as the corresponding capacities and peculiarities of the state protection policy in such a space. It also lists the powers and postulates of coordination to assure cybersecurity in this expanse for government offices, institutions, and citizens. At the same time, the abovementioned legal act doesn’t regulate the relevant matters concerning social networks and private electronic information resources on the Web.

Following the Law, communication systems of all kinds of ownership are subject to cybersecurity if they process national information resources, as well as if they are used in the interests of our country or local officials, as well as law enforcement agencies.

The main subjects of the national cybersecurity system in our state are:

- Ukrainian Police;
- Security service of Ukraine;
- State Service for Special Communications and Information Protection
- Ministry of Defence;
- National Bank;
- General Staff of the Ukrainian Armed Forces and intelligence agencies [8].

Cybersecurity actions are coordinated by the President of our state through the National Security and Defense Council headed by him. Within this organization, the National Cyber Security Coordination Center was established. It coordinates the actions of the security and defense area entities that assure cybersecurity and also suggests recommendations to the President on a cybersecurity strategy for the state [8].

Additionally, there is a government group for reacting to crisis events in Ukraine in the computer area - CERT-UA. This body is entrusted with the duties of maintaining a registry of incidents in the cybersphere, providing assistance in cyberattacks, teaching the basics of cyber defense through courses and seminars [8].

So, states, especially their responsible authorities in the field under study, need to monitor technological development and accumulate knowledge and skills to resist the development of digital crime at both the national and regional levels. After all, it is obvious that it is difficult to counter cybercrime exclusively at the national level, without active interaction with similar international organizations

that coordinate and provide assistance and counter criminal activities.

Thus, each state, including Ukraine, to effectively resist virtual cybercriminals, needs to actively develop a multi-level institutional cybersecurity system. It was it that would protect both state institutions and ordinary citizens of the state. According to D.N. Karpova, such a system should include various components, incl. increasing the level of digital literacy of the population, assistance in promoting individual methods of protecting personal data and mechanisms for countering, and preventing cyber threats [5, p. 48].

Conclusion. So, today most countries of the world are faced with cybercrime problems. In Ukraine, the corresponding law on cybersecurity has already been enacted, and the country is trying to use its potential to protect the rights and freedoms of its citizens from abuse in the cyber environment.

Nevertheless, the problem of the responsibility of Ukrainian state bodies and Ukraine itself for violation of its citizens' rights in the sphere of cybercrimes should be worked out in more detail at the legislative level.

A comprehensive program should be implemented with the purpose of combating cybercrime. It should be done through the involvement of both governmental bodies and the private sector of the Ukrainian economy. Within its framework such actions are needed:

- to organize international cooperation to coordinate the actions of special services;
- to adopt the most effective norms from the national legislation of other countries and, on their basis, develop additions to the existing regulatory legal acts to optimize national legislation and adapt it to new technical capabilities;
- to constantly update (to improve) the cybersecurity strategy at the national economic level;
- to organize the conditions and basis for interaction between law enforcement agencies, courts, and services to resist law violation шт the cyberspere;
- to actively involve in mutual work everyone interested in eliminating cybercrimes, namely law enforcement agencies, representatives from the economic sector of business and the academia community;
- to form a modern material base for the activities of services to resist cyber threats;
- to conduct as often as possible events to disseminate information about modern cyber threats among citizens of Ukraine to increase their cyber literacy.

So, today cyber attackers significantly harm not only the national economy but also organizations and citizens. Therefore, it is important to know about our rights in the cyber sphere, as well as about the responsibility of the public authorities for their violation and timely apply for the protection of the relevant rights and interests.

Література

1. Halder D., Jaishankar K. (2011). Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

2. Rouse M. Cybercrime / TechTarget. 2017. URL: https://searchsecurity. techtarget.com/ definition/cybercrime.

3. What Is Cybersecurity? / CISCO official website. 2019. URL: https://www.cisco.com/ c/en/ us/products/security/what-is-cybersecurity.html.

4. Бабаджанян К.А. Ответственность государства перед личностью как принцип правового государства. *Вестник Саратовской государственной юридической академии*. 2012. № 3. С. 36–41.

5. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение. *Власть*. 2014. № 8. С. 46-50.

6. Конституція України від 28 чер. 1996 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

7. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

8. Про основні засади забезпечення кібербезпеки України: Закон України від 9 трав. 2018 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

9. Про судоустрій і статус суддів: Закон України від 6 груд. 2016 р. № 1774-VIII. *Відо-*

мості Верховної Ради України. 2016. № 31. Ст. 545.

10. Рогозин В.Ю. Изменения в криминалистических характеристиках преступников в сфере высоких технологий. *Расследование преступлений: проблемы и пути их решения*. 2015. № 1 (7). С. 56–58.

11. Чекунов И.Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы. *Молодые ученые*. 2012. № 3. С. 178-186.

References

1. Halder D., Jaishankar K. (2011). Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

2. Rouse M. Cybercrime / TechTarget. 2017. URL: https://searchsecurity. techtarget.com/ definition/cybercrime.

3. What Is Cybersecurity? / CISCO official website. 2019. URL: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

4. Babadzhanjan K.A. Otvetstvennost' gosudarstva pered lichnost'ju kak princip pravovogo gosudarstva. *Vestnik Saratovskoj gosudarstvennoj juridicheskoj akademii*. 2012. № 3. S. 36–41.

5. Karpova D.N. Kiberprestupnost': global'naja problema i ee reshenie. *Vlast'*. 2014. № 8. S. 46-50.

6. Konstytucija Ukrai'ny vid 28 cher. 1996 r. *Vidomosti Verhovnoi' Rady Ukrai'ny*. 1996. № 30. St. 141.

7. Pro osnovni zasady zabezpechennja kiberbezpeky Ukrai'ny: Zakon Ukrai'ny vid 5 zhovt. 2017 r. № 2163-VIII. *Vidomosti Verhovnoi' Rady Ukrai'ny*. 2017. № 45. St. 403.

8. Pro osnovni zasady zabezpechennja kiberbezpeky Ukrai'ny: Zakon Ukrai'ny vid 9 trav. 2018 r. № 2163-VIII. *Vidomosti Verhovnoi' Rady Ukrai'ny*. 2017. № 45. St. 403.

9. Pro sudoustrij i status suddiv: Zakon Ukrai'ny vid 6 grud. 2016 r. № 1774-VIII. *Vidomosti Verhovnoi' Rady Ukrai'ny*. 2016. № 31. St. 545.

10. Rogozin V.Ju. Izmenenija v kriminalisticheskih harakteristikah prestupnikov v sfere vysokih tehnologij. *Rassledovanie prestuplenij: problemy i puti ih reshenija*. 2015. № 1 (7). S. 56–58.

11. Chekunov I.G. Kiberprestupnost': ponjatie, klassifikacija, sovremennye vyzovy i ugrozy. *Molodye uchenye*. 2012. № 3. S. 178-186.

В. В. Філінович

ПРОБЛЕМИ ПОРУШЕННЯ ПРАВ ЛЮДИНИ, СПРИЧИНЕНІ КІБЕРЗЛОЧИНАМИ, І СПОСОБИ ЇХ ПОДОЛАННЯ

Національний авіаційний університет
проспект Любомира Гузара, 1, 03680, Київ, Україна
E-mail: vvfilinovich@gmail.com

Метою *даного дослідження є критична оцінка та аналіз кіберзагроз і їх негативного впливу на права і свободи громадян України.* ***Методологічну основу*** *наукового дослідження склали традиційні методи типу філософського, світоглядного, загальнонаукового та окремі спеціальні методи. Проблему кібербезпеки та негативного впливу кіберзлочинів на права громадян також досліджували П. Сандлей, Дж. Льюїс, М. Роуз, Д. Гальдер, К. Джайшанкар і інші вчені.* ***Результатом*** *дослідження став аналіз наявних норм законодавчих актів України, які регулюють питання кібербезпеки в державі. Автор надає також перелік методів та шляхів реалізації комплексної програми боротьби із кіберзлочинністю в нашій державі. Так, вважається за необхідне ведення активного міжнародного співробітництва для координації дій особливих установ та організацій, організація якісних умов для плідної взаємодії правоохоронних органів, судів та інших організацій у сфері з протидії кіберзлочинності, формування інноваційної матеріальної бази, проведення заходів для підвищення рівня цифрової обізнаності українців тощо.*

Сучасні інформаційні технології середньостатична людина використовує щодня. Тому не дивно, що цифрове середовище наразі стало майданчиком для злочинних дій кіберзлочинців. Кіберпростір використовується ними для проведення кібератак проти окремих осіб, організацій і навіть цілих урядів та держав. Вказане становище ускладнюється тим, що для зазначеної незаконної діяльності не існує кодонів як фізичних, так і віртуальних. Але негативний вплив, спричинений такою діяльністю, загрожує усьому світу і, в першу чергу, правам та свободам людини і громадянина.

Автор вказує на те, що більшість країн світу стикаються з проблемою кіберзлочинності. В нашій державі вже прийнятий відповідний закон щодо кібербезпеки, і країна намагається використати свій потенціал для захисту прав і свобод своїх громадян від зловживань у цифровому просторі. Автор підкреслює, що питання про відповідальність державних органів і самої держави за порушення прав громадян у сфері кіберзлочинів слід опрацювати більш детально на законодавчому рівні. ***Дискусія*** *в статті плідно ведеться щодо шляхів вдосконалення національного законодавства у сфері кібербезпеки на прикладі нормативних актів інших країн. Як результат дослідження автор також надає перелік методів і дій, які необхідно вжити при боротьбі з наслідками кіберзлочинів та задля протидії їх вчиненню.*

Ключові слова: *кіберзлочинність; кібербезпека; кіберпростір; порушення прав людини; кіберсередовище; захист прав громадян у кіберпросторі; кібератака.*