UDC 346.7
DOI https://doi.org/10.24144/2788-6018.2023.06.55

ECONOMIC AND LEGAL FRAMEWORK FOR ENSURING CYBERSECURITY AS A PREREQUISITE FOR THE INTRODUCTION OF SPECIAL ECONOMIC REGIMES

Сєрєбряк С.В.,
кандидат юридичних наук, докторант,
Державна установа Інститут економіко-правових досліджень ім. В.К. Мамутова
Національної академії наук України
ORCID: 0000-0001-7207-594X

Sieriebriak S.V. Economic and Legal Principles of Cybersecurity as a Prerequisite for the Introduction of Special Economic Regimes.

The article conducts a scientific and practical study of the economic and legal aspects of the State policy in the field of cybercrime and its impact on business development in a particular region, country, etc. It is determined that the massive spread of cybercrime, the lack of effective mechanisms for combating economic crimes, and the leveling of conceptual approaches to creating an effective mechanism for legal support of the business environment development have a negative impact on the investment environment in particular and on ensuring sustainable development of the State as a whole. The author analyzes the regulatory and legal documents which form the legal basis of the mechanism for combating cybercrime, both at the international and national levels. The author identifies the weaknesses of the national system of legal regulation of cybersecurity. The author points out the sufficiency and fragmented nature of legislative support for cybersecurity and counteraction to the growth of economic crimes.

It is established that the significant vulnerability of Ukraine's information sphere is due to the excessive use of foreign-made material and technical means. It is emphasized that the international scale of the fight against cybercrime requires clarification and harmonization of national legislation in order to be able to cooperate with law enforcement agencies abroad. The article focuses on the low efficiency of Ukraine's current cybersecurity system and the urgent need to improve and optimize it. Achieving this will not only solve the problem of information space security, but also ensure the continuity and sustainability of Ukraine's economic development.

It is determined that one of the priority areas of work in the field of creating optimal conditions for business is the fight against computer crimes in the economic sphere. Among the main tasks in this area of activity is to counteract the legalization of shadow income. The analysis of money laundering schemes shows that organized crime is very interested in using the capabilities of electronic payment systems which allow for instant money transfers with almost complete anonymity of counterparties.

Key words: economic crime, cybersecurity, cybercrime, cyberattack, special economic regime.

Сєрєбряк С.В. Економіко-правові засади забезпечення кібербезпеки як передумова запровадження спеціальних режимів господарювання.

У статті проводиться науково-практичне дослідження економіко-правових аспектів державної політики у сфері кіберзлочинності та її впливу на розвиток бізнесу в тому чи іншому регіоні, країні тощо. Визначено, що масове розповсюдження кіберзлочинності, відсутність дієвих механізмів протидії економічним злочинам, нівелювання концептуальних підходів до створення ефективного механізму правового забезпечення розвитку бізнес-середовища негативно впливає на інвестиційне середовище зокрема та на забезпечення сталого розвитку держави в цілому. Проаналізовано нормативно-правові документи, що становлять юридичне підґрунтя механізму протидії кіберзлочинності, як на міжнародному, так і на національному рівні. Виявлено слабкі місця національної системи правового регулювання кібербезпеки. Вказується на достатність та фрагментарний характер законодавчого забезпечення кібербезпеки та протидії зростанню економічних злочинів.

Встановлено, що значна вразливість інформаційної сфери України сталась через надмірно широке використання матеріально-технічних засобів іноземного виробництва. Акцентовано увагу, що міжнародні масштаби боротьби з кіберзлочинністю передбачають уточнення і гармонізацію національного законодавства з тим, щоб мати можливість спільної співпраці з правоохоронними органами за кордоном.

Зосереджено увагу на низькій ефективності сучасної системи кібербезпеки України і першочерго-

ву потребу її удосконалення та оптимізації. Досягнення цього вирішить не тільки проблему безпеки інформаційного простору, але і забезпечить безперервність та сталість розвитку економіки України.

Визначено, що одним з пріоритетним напрямків роботи у сфері створення оптимальних умов для роботи бізнесу є боротьба з комп'ютерними злочинами у сфері економіки. Серед основних завдань на цьому напрямку діяльності необхідно назвати протидію легалізації тіньових доходів. Аналіз схем відмивання коштів свідчить про значну зацікавленість організованої злочинності у використанні можливостей електронних платіжних систем, які дозволяють здійснювати миттєві перекази коштів із забезпеченням практично повної анонімності контрагентів.

Ключові слова: економічний злочин, кібербезпека, кіберзлочин, кібератака, спеціальний режим господарювання.

Problem statement. The use of modern information technologies in governmental and non-governmental organizations, as well as in society as a whole, is now quite widespread. This leads to the growth of cybercrime and makes the issue of information security one of the most important. In addition to direct damage from possible cases of unauthorized access to information, its modification or destruction, informatization can become a source of serious threats to state security and human rights.

The involvement of computer technologies in more and more areas of state activity brings Ukraine closer not only to global standards and trends, but also to their negative consequences. The country's economy and security are increasingly dependent on technical infrastructure and its security.

Organizational and legal support for combating economic crime is an important component of the existence of a person, society, and the state in any country. In many countries, combating economic crime is recognized as an object of state policy, and therefore an object of public administration, which is formalized in public law. Economic crime is defined in the legal acts of many countries as a risk, a challenge, a threat to national security.

The growth of economic crime as a type of crime in the real and so-called virtual environment of society, including that which has transnational features, necessitates the need to increase proper scientific attention. Today, it is urgent to form, under the auspices of specialized international organizations, an appropriate computerized information resource (integrated database) on crime rates in the world, its individual regions and countries, based on the international classification of crimes for statistical, criminological and other human rights, law enforcement and security purposes, goals and objectives.

The state of development of this issue indicates that cybersecurity is not sufficiently defined in Ukraine, unlike international practice. Scientific, practical and comparative legal analyzes of the problematic issues of economic and legal support for the introduction of special economic regimes in the context of a constant increase in the number of economic crimes are important and relevant both in theoretical terms and in practical application, and are carried out by scholars and practitioners, including O. Bakalinska, O. Bakalinskyi, Y. Baturina, P. Bilenchuk, V. V. Vekhov, V. B. Vekhova, A. V. Voitsikhovsky, V. O. Golubeva, D. O. Hrytsyshen, M. D. Dikhtyarenko, I. O. Dragan, B. X. Toleubekova, V. S. Tsymbalyuk and others.

The purpose of the article is to study the economic and legal aspects of cybersecurity in terms of introduction of special economic regimes, to provide a systematic analysis of the State policy in the area of introduction of special economic regimes and the possibility of their introduction in the context of growing economic crimes and constant threats of cyber-attacks with a view to ensuring proper legal certainty of problematic issues, and to find effective organizational and legal forms, methods and ways of protecting the rights of economic entities.

Presentation of the main material. Cybercrime can be interpreted as a set of acts defined by criminal law committed in a particular territory or in relation to objects located therein over a certain period of time, committed in virtual space by means of destructive impact on computer systems, computer networks and computer data [1]. It is important to note that the profits from this criminal activity are quite significant. For example, according to a study by the international company McAfee, in 2008, profits from cybercrime reached 104 billion US dollars, while according to a bulletin published by the FBI in 2016, they exceeded 1 trillion dollars, which is ten times more profitable than arms trafficking and drug trafficking. Consequently, businesses lose almost the same (if not larger) amounts of money. Therefore, the fight against computer crime is one of the most important tasks of our time [2].

It should be emphasized that the effective fight against transnational computer crime and cyberterrorism requires close, fast, effective and functional international cooperation of all government agencies in the investigation of such crimes. Without a well-established mechanism of international cooperation in this area, it is impossible to ensure cybersecurity in any country in the world.

Ukraine took the first significant steps towards establishing international cooperation in combating cybercrime at the beginning of the XXI century, when on November 23, 2001, in Budapest, our

country, together with 30 other states, signed the European Convention on Cybercrime [3]. Representatives of the signatory countries, realizing the profound changes caused by the transition to digital technologies and the globalization of computer networks, concerned about the risk that computer networks and electronic information may be used to commit crimes, believing that effective fight against cybercrime requires close, rapid and effective, functional international cooperation in the investigation of such crimes, agreed on the need to take specific measures in each country [4]. The Convention provides for the granting of powers sufficient to effectively combat crimes in the field of information and telecommunications technologies both at the domestic and international levels. According to this document, the parties shall cooperate through the application of relevant international agreements on criminal matters concluded on the basis of uniform or reciprocal legislation, as well as domestic legislation, in order to investigate offenses related to computer systems and data and collect evidence in electronic form.

The next important step of Ukraine on the way to establishing interstate cooperation in the area under study is the ratification on September 7, 2005 of the said Convention with the Additional Protocol thereto of January 28, 2003, which provides for the granting of powers sufficient to effectively combat crimes in the field of information and telecommunications technologies both at the domestic and international levels; conclusion of agreements on effective international cooperation. In this regard, one of the urgent tasks of the state authorities and management of our country is to bring the existing mechanisms of international cooperation in line with the provisions of the above-mentioned Convention.

Ukraine has created and operates a fairly extensive system of information security and protection. There is a certain legislative framework consisting of the Laws of Ukraine «On Information», «On Protection of Information in Automated Information Systems», «On State Secrets», etc. There are a number of presidential decrees and resolutions of the Cabinet of Ministers of Ukraine that regulate specific areas of activity in the field of information protection.

One of the most recent steps in this direction was the adoption by the President of Ukraine on September 21, 2012 of the Law «On Amendments to the Law of Ukraine «On Ratification of the Convention on Cybercrime». According to this law, the Ministry of Internal Affairs of Ukraine becomes the only body authorized to create a round-the-clock contact network to provide emergency assistance in investigating cases related to cybercrime, as well as in identifying persons accused of it and collecting evidence for these cases [5].

The activities of international law enforcement agencies make a significant contribution to the development of international cooperation. For example, back in 1994, the General Secretariat of Interpol 7 recommended that member states of this organization establish a National Central Advisory Unit on Computer Crime in order to ensure that information from other countries was received by national special forces in a mobile and accessible form (language of communication, specific terms, crime codes, etc.), as well as to ensure the prompt exchange of such data between countries. In Ukraine, such a unit was established in 1996 on the basis of the Interpol National Central Bureau.

An analysis of the practice of detecting and investigating criminal cases in the field of high technology shows that the most common types of crimes related to the use of computer technology in modern Ukraine are: crimes in the field of computer and Internet technologies - 26%, crimes in the field of electronic payments or payment cards - 16%, crimes in the field of telecommunications - 11%, crimes in the field of using computer technology in the commission of traditional crimes - 47%.

In addition, the theft of the identification data of other persons has become an independent type of criminal activity, using which offenders gain access to other people's bank accounts, receiving free services of Internet providers and telecommunications operators. Such crimes are characterized by a high level of technical support, latency, organization, and interregional and international ties [6].

In modern conditions, computer crime is mostly organized and international in nature, based on the rapid development and use of telecommunication means of communication. About 62% of computer crimes are committed by organized groups, often in several countries. Computer crime is also characterized by a steady increase and improvement of the methods of committing crimes, each of which has many ways of implementation.

Undoubtedly, it is virtually impossible to solve such crimes and expose the perpetrators without the assistance of law enforcement agencies of partner countries. In order to ensure effective counteraction to high-tech crime, the Ministry of Internal Affairs of Ukraine has been taking organizational and practical measures to ensure effective counteraction to this modern type of transnational crime throughout the entire period of our country's independent development.

Analyzing the trends and dynamics of computer crime in Ukraine leads to the conclusion that the regions with the most developed information infrastructure, where the population widely uses telecommunication technologies (the Autonomous Republic of Crimea, Donetsk, Dnipro, Odesa, Lviv, Kharkiv) should be considered the most affected

by this phenomenon. The leader in this area was the city of Kyiv, where almost 60% of the entire Ukrainian Internet audience is located [7].

A characteristic feature of crimes committed through computer systems and telecommunication networks is their cross-border nature, so the disclosure and documentation of such illegal encroachments, as we have already noted above, is based on effective cooperation with law enforcement agencies of other states and international organizations specializing in combating cybercrime.

One of the most pressing issues today is the spread of fraudulent activities related to the advertising of so-called spyware, phone scanners, short text message interceptors, and programs for detecting the location of cellular terminals, which is gaining popularity among criminals due to the relative ease of committing such attacks.

International cooperation in preventing and combating cybercrime is not limited to contacts with foreign law enforcement agencies. In order to implement international standards in this area, the Department is currently actively developing cooperation with representatives of the Council of Europe and the European Union, other governmental and non-governmental organizations [8].

Another priority area of work in the field of creating optimal conditions for business is the fight against computer crimes in the field of economy. Among the main tasks in this area of activity is to counteract the legalization of shadow income. The analysis of money laundering schemes shows that organized crime is highly interested in using the capabilities of electronic payment systems, which allow for instant transfers of funds while ensuring almost complete anonymity of counterparties. Of particular interest in light of the problem is the fact that electronic payment systems are not classified as subjects of primary financial monitoring and therefore are not required to inform supervisory authorities of suspicious transactions, store information about transactions, and data that allows for customer identification.

In order to counteract the legalization of the proceeds of crime, the specially authorized bodies have established cooperation with the representative offices of the most widespread electronic payment systems in the Ukrainian Internet space and financial institutions that provide services to e-commerce entities and have data on fraud, interference with computer systems and other unlawful encroachments committed with the use of high technologies [9].

It should be noted that the existing domestic regulatory framework for combating cybercrime only partially meets the needs of the time and does not always cover all the key elements necessary for effective counteraction to cybercrime of all levels of complexity. Today, Ukraine has a number of laws and regulations at various levels covering the issues of cybersecurity. A number of intergovernmental legal acts recognize that cybercrime poses a threat not only to the national security of individual states, but also to humanity and the international order. Thus, it can be stated that the national regulatory framework in the field of information security operates with the definition of «cyberterrorism».

The separation of the concept of «cyberterrorism» as an independent one is one of the most controversial issues in the cybersecurity sphere. This is due, firstly, to the extreme politicization of the term, and secondly, to the need to clearly (and practically) define its key parameters so that they cannot be used to cover ordinary computer crimes or computer hooliganism. Today, in Ukraine, countering terrorism and combating its manifestations are carried out on the basis of the Law of Ukraine «On Combating Terrorism», which defines Terrorism is defined as «socially dangerous activity that consists in the deliberate, purposeful use of violence by taking hostages, arson, murder, torture, intimidation of the population and authorities or other attacks on the life or health of innocent people or threats of criminal acts in order to achieve criminal goals».

In addition, the same Law defines «technological terrorism» as «crimes committed for terrorist purposes with the use of nuclear, chemical, bacteriological (biological) and other weapons of mass destruction or their components, other substances harmful to human health, electromagnetic means computer systems and communication networks, including the seizure, disabling and destruction of potentially dangerous objects that directly or indirectly created or threaten to create a threat of an emergency as a result of these actions and pose a danger to personnel, the public and the environment; create conditions for accidents and man-made disasters» [10, p. 110] . Certain provisions of this definition include components that can be attributed to «cyberterrorism» («...the use of electromagnetic means, computer systems...»), but due to their lack of detail cannot be fully used in the practical work of law enforcement agencies.

Conclusions. Since no state can protect itself by taking measures at the national level alone, a comprehensive response to cybercrime requires harmonization of criminal legislation on cybercrime at the international level; development at the international level and implementation in national legislation of procedural standards that allow for effective investigation of crimes in global information networks, obtaining, examining and presenting electronic evidence, taking into account the cross-border issue; established cooperation of law enforcement agencies in the investigation of cybercrime at the operational level; a mechanism for

resolving jurisdictional issues in cyberspace. Thus, international cooperation is key to eliminating the legal vacuum that exists between the development of information technologies and the response of legislation to them. Experience shows that the process of developing measures at the international level is a complex problem in itself. However, it is the only way to ensure the safety of users and the state from electronic attacks, as well as to effectively investigate and prosecute cybercrime.

Ensuring cybersecurity in the context of special business regimes is quite important. When it comes to the arrival of investors, including foreign ones, in a certain region or in a certain sector of the economy, the state's urgent task is to ensure their stable operation and business development. One of the most serious obstacles in the modern development of society for the full development of business is the threat of cyberattacks on a particular enterprise. This problem is generally quite global and international. The threat is the loss of business in general, as well as potential loss of business reputation or loss of intellectual property rights. This problem must be resolved in the economic and legal sphere in the near future, as Ukraine's post-war recovery is impossible without investing in its economy, developing its business environment, and creating new jobs.

REFERENCES:

1. Буяджи С.А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект: дис. … канд. юрид. наук: 12.00.01. Київ, 2018. 203 с.
2. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. Аналітична записка: URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/problemi-chinnoi-vitchiznyanoi-normativno-pravovoi-bazi-u-sferi.
3. Конвенція про кіберзлочинність від 23.11.2001 р.: URL: https://zakon.rada.gov.ua/laws/show/994_575#top.
4. Голубев В.А. Проблемы борьбы с преступлениями в сфере использования компьютерных технологий: [учеб. пособие] / Голубев В.А., Гавловский В.Д. , Цимбалюк В.С.; под общ. ред. Р.А. Калюжного. Запорожье: ЗИГМУ, 2002. 292 с.
5. Про внесення змін до Закону України "Про ратифікацію Конвенції кіберзлочинності: Закон України 21 вересня 2010 року № 2532-VI URL: https://zakon.rada.gov.ua/laws/show/2532-17#Text.
6. Войціховський А.В. Міжнародне співробітництво у боротьбі з кіберзлочинністю. Портал: Національна бібліотека імені В.І. Вернадського. URL: http://www.archive.nbuv.gov.ua/portal/.../PB-4_26.pdf.
7. Гвоздецький В. Проблеми міжнародного співробітництва в протидії злочинності у сфері високих технологій. Вісник Академії управління МВС. 2007. № 2-3. С. 6.
8. Матеріали брифінгу в МВС України щодо новітніх напрацювань органів внутрішніх справ у боротьбі з кіберзлочинністю URL: mvs.gov.ua.
9. Матеріали брифінгу в МВС України щодо новітніх напрацювань органів внутрішніх справ у боротьбі з кіберзлочинністю URL: mvs.gov.ua.
10. Бабанін С.В. Комп'ютерні злочини за кримінальним законодавством України, США та Польщі / С.В. Бабанін / Співпраця поліції/міліції зі службами безпеки Інтернетсайтів (аукціонів, соціальних мереж тощо) у боротьбі з інтернет-злочинністю на підставі національного законодавства та законодавства, яке діє у Європейському Союзі: тези доповідей міжнародної науково-практичної конференції (м. Хмельницький, 16–17 листопада 2010 року) / МВС України; УМВС України в Хмельницькій області.Хмельницький: УМВС, 2010. 100 с.