УДК 342.951
DOI https://doi.org/10.32840/1813-338X-2020.2.17

В. С. Сірко
кандидат юридичних наук,
старший викладач кафедри адміністративного права та процесу
Одеського державного університету внутрішніх справ

ОРГАНІЗАЦІЙНО-ПРАВОВІ ПИТАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Встановлено, що стрімке проникнення в повсякденне життя комп'ютерної техніки й комп'ютерних технологій, що сприяє розвитку інформаційних, телекомунікаційних та інформаційно-телекомунікаційних мереж, поставило перед суспільством питання про необхідність захисту від протиправних посягань як особистої інформації, так і найважливіших сегментів національної безпеки – фінансового, економічного й інформаційного.

Узагальнено, що кіберзлочинності разом із загальними ознаками злочинності властиві й специфічні форми прояви й ознаки, що «вигідно» відрізняють її від «традиційних» видів злочинності: як правило, вона має міжнародний характер (виходить за межі однієї держави); наявні істотні труднощі у визначенні місця скоєння злочину; мають місце слабкі зв'язки між рівнями й ланками в системі доказів; неможливість спостереження та фіксації доказів злочину візуально; широке використання засобів шифрування інформації; відсутність механізмів контролю; автоматизація та швидкість використання «злочинної» інформації; анонімність у мережі Інтернет.

Кіберзлочинність містить різні види злочинів, що здійснюються за допомогою комп'ютера й в мережі Інтернет. Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі й інша особиста інформація як фізичних осіб, так і бізнесу й державного сектору. Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні.

В Україні до кіберзлочинів відносять порушення авторського права й суміжних прав; шахрайство; доступ до банківських рахунків платіжними картками й іншими засобами, обладнання для їх виготовлення; ухилення від сплати податків, зборів (обов'язкових платежів);, незаконні дії з документами на переказ; ввезення, виготовлення, збут і розповсюдження порнографічних предметів; незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю.

Об'єктом кіберзлочинів може стати будь-який користувач інтернету.

Ключові слова: *інформаційно-телекомунікаційні системи, кіберзлочинність, комп'ютерні злочини, ознаки кіберзлочинності, поняття злочинності, протидія.*

Постановка проблеми. Нині складно собі уявити сферу діяльності, в якій не використовується комп'ютерна техніка, комп'ютерні та телекомунікаційні мережі. Жоден складний технологічний процес не може існувати без високих (інформаційних) технологій, соціальні мережі з кожним роком залучають мільйони користувачів, кожен з яких довіряє мережі частину свого особистого життя [1, с. 46]. Однак і ця сфера «віртуальних» суспільних відносин не позбавлена вразливості.

У ній шляхом знеособленості користувачів часто знаходять зображення найбільш ниці прояви особистості внаслідок необізнаності користувачів про наявні можливості мережі, вона проста й доступна для злочинних посягань. Це насамперед викликано тим, що глобальні цифрові технології відкривають нові можливості для діяльності злочинців, сприяють поширенню злочинів у сфері порушення прав інтелектуальної власності, створюють умови для поширення продукції порнографічного характеру, матеріалів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію, спрощують можливість придбання і збуту наркотичних і психотропних засобів, зброї тощо.

Аналіз останніх досліджень і публікацій. Комп'ютерні злочини й кіберзлочини деякі вчені трактують як різні види (групи) злочинів у сфері високих комп'ютерних технологій, класифікація яких здійснювалася за різними ознаками.

Водночас ознакою для «віднесення» окремих злочинів у сфері високих технологій до комп'ютерних в загальному вигляді є знаряддя скоєння злочину – комп'ютерна техніка, а ознакою для виділення кіберзлочинів – специфічне середовище скоєння злочинів – кіберпростір (середовище комп'ютерних систем і мереж). Якщо розглядати групу злочинів, об'єднану в окремий розділ Кримінального кодексу України [4] – «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» у відриві від інших форм прояву злочинної поведінки з використанням комп'ютерної техніки й високих технологій, водночас допускаючи, що вони не перебувають (не включені) в єдину мережу, то така класифікація має сенс. Їх залученість у мережі різних рівнів і створює можливість для здійснення діянь, що характеризуються підвищеною (кримінально караною) суспільною небезпекою.

Метою статті є дослідити організаційно-правові питання протидії кіберзлочинності.

Виклад основного матеріалу. Кіберзлочинності, разом із загальними ознаками злочинності, властиві й специфічні форми прояви й ознаки, що «вигідно» відрізняють її від «традиційних» видів злочинності:

– як правило, вона має міжнародний характер (виходить за межі однієї держави);

– наявні істотні труднощі у визначенні місця скоєння злочину;

– наявні слабкі зв'язки між рівнями й ланками в системі доказів;

– неможливість спостереження та фіксації доказів злочину візуально;

– широке використання засобів шифрування інформації;

– відсутність механізмів контролю; автоматизація та швидкість використання «злочинної» інформації;

– анонімність в мережі Інтернет.

Виокремити напрями протидії кіберзлочинності дуже складно через багатогранність цього соціального явища [2, с. 34–35]. Відзначимо два основних напрямки. До першого напряму доцільно віднести попередження кіберзлочинності, що передбачає створення, сертифікацію, ліцензування і впровадження необхідних засобів технічного і програмного захисту інформації; створення спеціалізованих організаційних структур організацій і служб кібербезпеки, спрямованих на забезпечення надійного функціонування засобів захисту, генерація ключів і паролів, контроль щодо їх використання, зміні й знищенню; підготовку кваліфікованих кадрів для правоохоронних органів.

Другий напрямок протидії кіберзлочинності містить виявлення і попередження кіберзлочинів. Нині проблема кінцевого вирішення організації ефективної взаємодії та координації суб´єктів протидії кіберзлочинності знаходиться на стадії завершення. Саме багатогранність суб´єктів протидії кіберзлочинності передбачає багаторівневу координацію їх діяльності.

Розглянемо детальніше систему суб´єктів протидії кіберзлочинності в Україні. З 1991 року при Генеральному секретаріаті Інтерполу створюється Робоча група щодо проблем комп´ютерної злочинності, яка спрямовує свою увагу на розв'язання проблем міжнародного співробітництва під час розслідування комп´ютерних злочинів. Як наслідок в Україні створюється Національний центральний консультативний пункт щодо проблем комп´ютерної злочинності [3]. Це дозволило систематизувати матеріали про законодавче регулювання та організаційний досвід боротьби з кіберзлочинністю в різних країнах, підготувати низку аналітичних звітів і публікацій на цю тематику, ознайомити співробітників МВС України, прокуратури, суду з новим видом злочинної діяльності й внести суттєві зміни в кримінальне законодавство.

Протягом останніх п'ятнадцяти років у структурах СБУ і МВС створюються різні департаменти й відділи, основне завдання яких полягає в боротьбі з правопорушеннями у галузі інтелектуальної власності й високих технологій, захисту інформації та інформаційних ресурсів країни.

5 листопада 2015 року була створена нова Кіберполіція, яка є структурним підрозділом Національної поліції України [5]. Основною ціллю кіберполіції є реформування і розвиток підрозділів МВС України, які забезпечують підготовку і функціонування висококваліфікованих спеціалістів експертних, оперативних і слідчих підрозділів поліції, що здійснюють боротьбу з кіберзлочинністю і здатні застосовувати новітні технології в оперативно-службовій діяльності.

До основних завдань кіберполіції належать:

– реалізація державної політики у сфері боротьби з кіберзлочинністю;

– протидія кіберзлочинності;

– своєчасне інформування громадськості про скоєння нових кіберзлочинів;

– впровадження програмних засобів для систематизації та аналізу інформації про кібервипадки, кіберзагрози й кіберзлочини;

– реагування на запити іноземних партнерів, що надходять каналами Національної цілодобової мережі контактних пунктів;

– участь у підвищенні кваліфікації співробітників поліції у сфері застосування комп´ютерних технологій для боротьби з кіберзлочинністю;

– участь у міжнародних операціях і взаємодія в режимі реального часу; забезпечення функціонування мережі контактних пунктів між різними країнами світу.

Висновки і пропозиції. Роблячи підсумок, відзначимо, що протидія кіберзлочинності полягає в трьох основних напрямках: попередження кіберзлочинності, загальна організація боротьби з кіберзлочинністю, правоохоронна діяльність, спрямована на виявлення, попередження та розкриття кіберзлочинів, застосування кримінальної відповідальності й покарання осіб, що скоїли кіберзлочин. Пріоритетним напрямком є також організації взаємодії та координації зусиль правоохоронних органів, спецслужб, судової системи, забезпечення активізації міжнародного співробітництва в цій сфері.

Список використаної літератури:

1. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія. Київ : КИТ, 2010. 408 с.
2. Голубєв В.О. Розслідування комп'ютерних злочинів : монографія. Запоріжжя : Гуманітарний університет «ІДМУ», 2003. 296 с.
3. Гуцалюк М.В. Протидія комп'ютерній злочинності. URL: http://www.pravo.vuzlib.org/book_z726_pa ge_24.html.
4. Кримінальний кодекс України : Закон України від 23 липня 2020 р. № 2341-III / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2341-14/
5. Про Національну поліцію: Закон України від 02 липня 2015 р. № 580-VIII / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/580-19.

Sirko V. S. Organizational and legal issues of countereaction to cybercrime

It has been established that the rapid penetration of computer technology and computer technologies into the daily life that promotes the development of information, telecommunication and information and telecommunication networks, has raised the question for the society about the necessity for protection against illegal infringement of both personal information and the most important segments of the national security such as financial, economic and informational.

It is generalized that some scientists interpret computer crimes and cybercrimes as different types (groups) of crimes in the sphere of high computer technologies, classification of which has been carried out due to different features. Herewith, the feature for the "attribution" of separate crimes in the field of high technology to computer crimes in their general form is the tool for committing a crime that is computer technology. The feature to define a cybercrime is a specific crime environment that is cyberspace (an environment of computer systems and networks). It has been summarized that if we consider a group of crimes, united into a separate section of the Criminal Code of Ukraine. This section is called "Crimes in the field of use of electronic computers (computers), systems and computer networks and telecommunication networks". In contrast to other forms of manifestation of criminal behavior with the use of computer technology and high technology, while assuming that they are not (not included) in a single network, this classification makes sense. It has been stated that their involvement into the network of different levels namely creates an opportunity for carrying out actions that are characterized by increased (criminally punished) social danger.

It has been generalized that cybercrime, along with the general features of crime, has inherent and specific forms of manifestation and features that "favorably" distinguish it from "traditional" types of crime. As a rule, it has international character (beyond the borders of one state), and there are significant difficulties in determining the crime scene. Moreover, there are weak connections between levels and links in the system of evidence, as well as inability to observe and record evidence of the crime visually. Finally, the other problems are widespread use of different means of encryption, lack of control mechanisms, automation and speed of use of "criminal" information and anonymity on the Internet.

Cybercrime includes various types of crime committed on a computer and on the Internet. The object of cybercrime is personal data, bank accounts, passwords and other personal information of both individuals and businesses and the public sector. Cybercrime is a threat not only nationally but also globally.

In Ukraine, cybercrime includes copyright and related rights violations, fraud, payment cards and other means of access to bank accounts, equipment for their production; evasion of taxes, fees (mandatory payments), illegal actions with documents for transfer, import, production, sale and distribution of pornographic items, illegal collection for the purpose of use or use of information constituting a commercial or banking secret.

The object of cybercrime can be any Internet user.

Key words: *information and telecommunication systems, cybercrime, computer crimes, features of cybercrime, definition of crime, counteraction.*