УДК 343.3/7
DOI 10.33244/2617-4154.2(9).2022.195-203

Н. А. Лугіна,
канд. юрид. наук, доцент
e-mail: natali.lugina7@gmail.com
ORCID ID 0000-0001-6005-2943;
А. М. Бондаренко,
Державний податковий університет
e-mail: bondarenkoa034@gmail.com
ORCID ID 0000-0003-2493-8557

ПРАКТИЧНІ АСПЕКТИ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИННОСТІ – ЄВРОПЕЙСЬКИЙ ДОСВІД

У статті досліджено особливості кримінальних правопорушень у сфері інформаційно-телекомунікаційних технологій, а також звернуто увагу на основні проблеми щодо їх виявлення, розкриття та розслідування. Акцентовано увагу на досить великі масштаби розповсюдження кіберзлочинності, не тільки в Україні, а й в цілому – світовій спільноті. Проаналізовано напрями міжнародної взаємодії у сфері протидії кіберзлочинності, що зі свого боку ґрунтуються на міжнародних нормативно-правових актах. Взято до уваги певний досвід боротьби європейських держав, зокрема США, Канади, Франції, Великої Британії. Адже одним із пріоритетних напрямів удосконалення вітчизняної правової системи є саме впровадження міжнародних ідей та концепцій. Крім того, процес становлення цілісної системи правового регулювання боротьби з таким негативним явищем, як кіберзлочинність, не є можливим без урахування досягнень та прогалин, які були допущені іноземними державами у процесі формування цього інституту. Також існує необхідність вивчення і впровадження досвіду зарубіжних країн щодо організації та ефективного функціонування підрозділів боротьби з кіберзлочинністю.

У період глобалізації швидкий розвиток інформаційних технологій, нових систем комунікацій і комп'ютерних мереж супроводжується зловживанням цими технологіями зі злочинними намірами. Тому є не менш важливим також можливість оперувати і розуміти, що собою являє таке поняття, як «кібербезпека». Під кібербезпекою розуміється насамперед швидке реагування на загрози всередині мережі «Інтернет». Адже аналіз статистики показує, що в більшості випадків об'єктами кібератак стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій.

Ключові слова: *інформація, розслідування кіберзлочинів, європейський досвід, протидія кіберзлочинності в суспільному вимірі, правові механізми взаємодії, глобальна мережа, Конвенція по боротьбі з кіберзлочинністю.*

Метою цього дослідження є теоретичне та практичне обґрунтування поняття кіберзлочинності, її існування як суспільного явища. Аналіз боротьби з цим явищем у європейських країнах.

Постановка проблеми. У сучасному світі досить складно переоцінити суспільну шкідливість кіберзлочинності, аналізуючи такі її характеристики, як транснаціональність, латентність, висока динамічність темпів зростання та трансформацій, негативність та масштабність наслідків тощо. Варто зауважити, що в 2014 році в середньому кожний п'ятий житель Європи зіткнувся з певним проявом кіберзлочинності. Комп'ютерне піратство, шахрайство, хакерство та вже досить новітній прояв кіберзлочинності – кібертероризм міцно закарбувались у суспільній свідомості, як особливо небезпечні явища, перед якими можуть опинитися беззахисними як окремі громадяни, так і суспільство і держава в цілому. Саме тому кіберзлочинність уже набула масштабів загрози безпеці на міжнародному рівні і стала одним з основних інструментів державної та міжнародної діяльності.

На сьогодні комп'ютерні правопорушення – це одна з найбільш поширених груп суспільно небезпечних посягань, динаміка яких невпинно зростає. Це зумовлено прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки. Варто наголосити на тому, що в українському законодавстві цьому питанню приділена увага, а саме: новий Кримінальний кодекс України вперше передбачив окремий розділ про ці КП – розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж»; двічі положення цього розділу змінювалися та доповнювалися, це свідчить про актуальність цієї проблеми в суспільстві, а також уваги й аналізу на практиці.

Аналіз останніх досліджень і публікацій. Сучасні теоретичні та прикладні аспекти здійснення протидії кіберзлочинності та кібершахрайтву розглядалися провідними вітчизняними науковцями: М. О. Будаковим, В. М. Бутузовим, М. М. Галамбою, Р. А. Калюжним, В. В. Коваленко, Я. Ю. Кондратьєвим, Б. А. Кормичем, Ю. Є. Максименко, А. І. Марущаком, Г. В. Новицьким, В. І. Прокопенком, С. С. Рогульським, В. Г. Ротанем, М. І. Хавронюком та іноземними фахівцями А. Робертом, К. Осакве, Т. Блентаном, Д. Банісаром та ін.

Виклад основного матеріалу. Донедавна рівень кіберзлочинності в нашій країні був мінімальним – це зумовлено тим, що розвиток інформаційних технологій знаходився на досить низькому рівні, порівнюючи його з розвиненими країнами світу. Проте у вирі останніх років можемо спостерігати зовсім протилежне. Україна сьогодні – країна з високим рівнем безробіття, обмеженими можливостями працевлаштування, проте із наявністю молодого покоління, яке зі свого боку має достатньо амбіцій і прагнення отримати кошти, вдається до кібератак і часто уникає за

це покарання. В Україні відсутня офіційна державна статистика, яка містила б відомості про кіберзлочини, що негативно позначається на запобіжних заходах, які мають частковий характер і при цьому призводять до уповільнення протидії та боротьбі з таким видом суспільно небезпечних діянь. Серед причин зазначеного, зокрема, те, що терміном «кіберзлочинність» (визначений лише 2017 р. у Законі України «Про основні засади забезпечення кібербезпеки України») охоплюється широке коло правопорушень, ускладнюючи тим самим розробку системи типології або класифікації кіберзлочинності [6, с. 69].

Кіберзлочинність має природу транскордонного явища та дозволяє значній кількості вчених вказувати на те, що для кіберзлочинів є притаманним максимальний рівень латентності. Варто розглянути, які фактори латентності наявні для кіберзлочинів:

– складність механізму вчинення цих кримінальних правопорушень поєднана з досить різноманітними сферами та наслідками їх вчинення, а також «комп'ютерною безграмотністю» більшості потенційних жертв кіберзлочинів, адже їх насамперед вони нехтують власною безпекою;

– негативна поведінка жертв (очевидців) правопорушення, така собі бездіяльність – не звернення жертви та осіб, яким відомо про наявні ознаки вчинення кіберзлочинності, до правоохоронних органів і неповідомлення про факт вчинення кіберзлочину;

– суттєві недоліки в роботі правоохоронних органів щодо повільного реагування або ж взагалі залишення без уваги – звернення та повідомлення про кіберзлочини [7, с. 646–650].

Одним з найперших і можливих до втілення підходів боротьби з кіберзлочинністю в широкому аспекті є напрацювання і стандартизація відповідної нормативно-правової бази. На міжнародному рівні першими документами у цій сфері стали Конвенція про кіберзлочинність, прийнята Радою Європи 23 листопада 2001 р. [4], та Додатковий протокол до Конвенції, направлений на боротьбу з розповсюдженням через комп'ютерні мережі інформації расистського і ксенофобського характеру від 28 січня 2003 р. [3]. Прийняття цих нормативно-правових актів дало початок фундаменту у сфері захисту свободи, безпеки і прав людини в мережі «Інтернет» не тільки на регіональному рівні, оскільки Конвенція відкрита для підписання державами, які не є членами Ради Європи.

Під поняттям «кіберзлочини» розуміємо кримінальні правопорушення, які передбачені розділом XVI КК України («Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку»), та зареєстровані кримінальні провадження із кваліфікуючою відміткою в картці про кримінальне правопорушення – «з використанням високих інформаційних технологій і телекомунікаційних мереж» [5].

Глобальна всесвітня мережа «Інтернет», що об'єднала мільйони комп'ютерів, які розташовані в різних країнах, і відкрила широкі можливості для отримання та обміну інформації, усе частіше використовується у злочинних цілях. Станом на сьогодні разом з основними функціями перед правоохоронними органами постало нове завдання

попередження і розслідування правопорушень у сфері використання комп'ютерних технологій – «кіберзлочинів». Поняття кіберзлочину є досі незвичним для правоохоронних органів, проте злочинні дії, в яких використовується глобальна комп'ютерна мережа «Інтернет», містять у собі велику суспільну небезпеку. Транснаціональний характер злочинності з використанням комп'ютерної мережі дає підстави вважати, що розробка спільної політики з основних питань повинна бути частиною будь-якої стратегії боротьби з кіберзлочинністю. Також певною мірою чинником, що сприяє зростанню цього нового виду злочинів, можна вважати відсутність належної взаємодії національних правоохоронних органів у питаннях попередження та розслідування таких видів правопорушень.

Крім дослідження досвіду всієї європейської спільноти, доцільно провести паралелі щодо провідних держав Союзу. Почнемо з аналізу Франції, в якій правове регулювання боротьби з кіберзлочинністю має свою специфіку, яка є достатньо дієвою. Врахуємо той факт, що саме Франція одна з перших держав в Європі, яка прийняла кардинальні міри щодо посилення ролі держави в регулюванні кіберпростору. Отже, на сьогодні в цій державі законодавцями було виокремлено такі форми кіберзлочинності:

– суспільно-небезпечні діяння, які зі свого боку пов'язані з незаконним та несанкціонованим тиражуванням комп'ютерного обладнання та програмного забезпечення, а також незаконним втручанням у роботу автоматизованої системи обробки даних, проникнення на сайти та створення на них недостовірної інформації, а також розповсюдження шкідливих програм тощо;

– розповсюдження сайтів, на яких присутня дитяча порнографія, збут наркотичних засобів, прекурсорів, расистської, ксенофобської або антисемітської спрямованості, інформації про тероризм, замахи на приватне життя, особисту недоторканість особи, повалення конституційного ладу, а також реклама, яка несе в собі шахрайські цілі [1, с. 68].

Варто зауважити, що французький досвід є актуальним для втілення його в Україні, враховуючи недосконалість розуміння і формулювання сутності поняття «кіберзлочинність». Можемо побачити, що правове регулювання першої форми кіберзлочинності Франції здійснюється в Україні на середньому рівні розділом XVI Кримінального кодексу України, а досвід регулювання другої форми – критично на низькому рівні, тому потребує детального аналізу та впровадження дієвих засобів боротьби і запобігання на практиці.

Щодо Сполучених Штатів Америки (далі – США), – це одна з перших держав, яка зазнала негативного впливу кіберзлочинності, розробила відповідні норми щодо усунення цього явища. А також у США протидія досліджуваному виду злочинності покладена на Федеральне бюро розслідування, в складі якого створено Центр скарг на інтернет-злочинність. Вказаний Центр приймає інтернет-скарги про злочини від фактичної жертви або від третьої сторони в онлайн режимі. Для подання скарги необхідно надати таку інформацію:

– ім'я жертви, адреса, телефон та електронна пошта;

– інформацію про фінансові операції (наприклад, інформацію про обліковий запис, дату здійснення операції та суму);

– ім'я суб'єкта, адресу, телефон, електронну адресу, вебсайт та IP-адресу;

– конкретні подробиці про те, як громадянин став жертвою злочину;

– заголовки електронної пошти;

– будь-яку іншу важливу інформацію, яку громадяни вважають необхідною для розгляду скарги [9, с. 165]. Водночас на сайті ФБР постійно оновлюються списки найбільш розповсюджених видів інтернет-шахрайств, фізичних та юридичних осіб, які підозрюються або підозрювались у вказаних правопорушеннях, способи відсторонення від інтернет-шахраїв, списки шкідливого програмного забезпечення на комп'ютерну та мобільну техніку.

Крім того, звернемо увагу на систему органів влади, що борються з кіберзлочинністю:

– кіберкомандування США (USCYBERCOM);

– команда з готовності до надзвичайних ситуацій США (CERT);

– відділ комп'ютерної злочинності й інтелектуальної власності (CCIPS) [9 с. 136–140].

Отже, як бачимо, для того щоб в Україні на сьогодні існував той самий орган – Департамент кіберполіції Національної поліції України, який намагається відійти від кіберзлочинності, повинен бути представлений у правоохоронному просторі, однак, на превеликий жаль, його існування нині є неможливим. У США таких рівнів боротьби та взаємодії між органами є три. Тому маємо за приклад боротьбу з кіберзлочинністю, що досягає ефективних результатів.

Заслуговує на увагу досвід боротьби з кіберзлочинністю Великої Британії, у якій запроваджено Модель обміну інформацією (Information Exchange Model) між урядовими установами і приватним сектором на принципах «Chatham House» (цей процес означає, що можна передавати і використовувати інформацію, яка була почута на зустрічах про виявлені атаки, втрату інформації тощо, але категорично заборонено вказувати, хто є її автором і де відбувся кіберінцидент). Координацію діяльності спільноти, організацію зустрічей, управлінську функцію забезпечує Центр із захисту національної інфраструктури (Centre for the Protection of National Infrastructure, CPNI – спеціально уповноважений орган з питань захисту критичної інфраструктури). CPNI створює канали, якими дані щодо обміну інформацією передаються в інші країни, зокрема, з цією метою створено мережу обміну інформацією з безпеки між Великою Британією і США [10, с. 194].

Правоохоронні органи Великої Британії під час боротьби з кіберзлочинністю також залучають спеціалізовані служби, які надають послуги інформаційної безпеки, при цьому співпрацюючи як з державними, так і з комерційними організаціями, для прикладу, WARP (Warning, Advice and Reporting Point) – сервісною службою, завдяки якій, зокрема, розкриваються тенденції кіберзлочинності [12].

Досвід Канади у сфері боротьби з кіберзлочинністю є не менш дієвим, ніж в інших цивілізованих державах. Зокрема, одним із важливих напрямів діяльності поліції Канади є боротьба з комп'ютерними і телекомунікаційними кримінальними правопорушеннями, розслідуванням яких займається підрозділ Королівської канадської

кінної поліції (федеральної поліції, КККП) з боротьби з комп'ютерною злочинністю, оперуючи аналізом даних канадського поліцейського інформаційного центру та співпрацюючи з іншими країнами. Діяльність підрозділу спрямована на розслідування та розкриття злочинів, пов'язаних з комп'ютерами і телекомунікаціями [4, с. 113]. Секція захисту інформаційних технологій забезпечує захист федеральних державних комп'ютерних центрів, приватного сектору, дає консультації, готує персонал для роботи зі здійснення комп'ютерного захисту.

Працівники цього підрозділу надають допомогу поліцейським у проведенні розслідувань злочинів, пов'язаних із комп'ютерними системами. Враховуючи, що інформаційна система дозволяє передавати повідомлення від одного терміналу до іншого майже негайно, у Канаді діє близько 2 500 точок доступу, до яких входять близько 1 285 федеральних і провінційних поліцейських відділень. 1 180 підрозділів спеціалізованих відділів КККП підключені до ліній системи [2, с. 48]. Безперечно, цей напрям діяльності поліції є важливим, адже економічні втрати вже досягли колосальних масштабів та і взагалі деякі правопорушники, створюють організовані групи, які мають на меті шкодити суспільству та знижувати рівень економіки країни. Водночас потрібно визнати, що канадське законодавство щодо визначення комп'ютерної злочинності потребує вдосконалення. Враховуючи, що завдання, які стоять перед підрозділами поліції з боротьби з комп'ютерною злочинністю, мають міжнародний характер і не є специфічними для Канади, проте вони активно співпрацюють з іншими країнами та Інтерполом з метою вдосконалення законодавства у цьому напрямі.

Висновки. Отже, варто зазначити, що процес боротьби з таким негативним явищем, як кіберзлочинність, досить складний і тривалий. Процес, який потребує значної уваги з боку органів влади, а також вимагає міждержавного підходу до протидії, результативність якого недосяжна без використання європейського досвіду. Маємо використовувати досвід країн, що вже мають досить серйозні напрацювання у сфері забезпечення інформаційної безпеки.

Ефективна боротьба з кіберзлочинністю вимагає розвиненої організаційної структури. Необхідними змінами в законодавстві для протидії протиправним посяганням на електронні інформаційні ресурси має бути закріплення механізму оперативного втручання і блокування певного неприйнятного потоку інформації та впровадження особливих умов проведення таких слідчих дій, як обшук і арешт електронних доказів.

Безумовно, варто також забезпечити проведення навчань (тренінгів) для співробітників органів прокуратури та суддів з метою їх фахової готовності до представництва інтересів держави і розгляду проваджень щодо кіберзлочинів, зокрема у частині порядку збирання цифрових доказів, їх передачі та зберігання. Це сприятиме розумінню співробітників органів прокуратури та суддів техніко-юридичних особливостей проваджень щодо кіберзлочинів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бутузов В. М. Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп'ютерній злочинності. *Боротьба з організованою злочинністю і корупцією (теорія та практика)*. 2019. Вип. 19. Оновлено 236 с.

2. Варунц Л. Д. Досвід організації діяльності Королівської канадської кінної поліції та шляхи його використання в Україні: дис. … канд. юрид. наук: 12.00.07 Д. 2018. 203 с.

3. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи: від 28 січ. 2003 р.; ратиф. Україною 21 серп. 2006 р. URL: http://zakon.rada.gov.ua/laws/show/994_687

4. Конвенція Ради Європи про кіберзлочинність: від 23 листоп. 2001 р. ратиф. Україною 7 верес. 2005 р. *Офіційний вісник України.* 2007. № 65. Ст. 2535.

5. Кримінальний кодекс України. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131.

6. Куракін О. М. Структура механізму правового регулювання. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2015. Вип. 35. 546 с.

7. Манжай О. В. Проблеми нормативно-правового забезпечення боротьби з кіберзлочинністю в Україні. *Форум права.* 2017. № 1. С. 646–650.

8. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і Безпека*. 2017. № 2. 469 с.

9. Марков В. В. Статистичне дослідження показників кіберзлочинності: методологічний аспект. *Право і безпека.* 2018. № 2. 367 с.

10. Сень Р. Ю. Досвід іноземних країн у сфері розслідування кіберзлочинів. Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності. Харків. 201 с.

11. Scams and Safety. Internet Fraud. URL: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud (in En.).

12. Warning, Advice and Reporting Point (WARP). URL: https://www.warpnetwork.org/services.html

REFERENCES

1. Butuzov V. M. International experience: the initiative of French law enforcement agencies to combat computer crime. *Fight against organized crime and corruption (theory and practice).* 2019. vol. 19. Updated 236 p.

2. Varunts L. D. Experience in the organization of the activities of the Royal Canadian Mounted Police and ways of its use in Ukraine: diss. Ph.D. law Sciences: 12.00.07 D. 2018. 203 p.

3. Additional Protocol to the Convention on Cybercrime, which concerns the criminalization of acts of a racist and xenophobic nature committed through computer

systems: dated January 28. 2003; ratification Ukraine on August 21 2006. URL: http://zakon.rada.gov.ua/laws/show/994_687

4. Council of Europe Convention on Cybercrime: dated November 23. 2001. Ratif. Ukraine on September 7. 2005. *Official Gazette of Ukraine.* 2007. No. 65. Art. 2535.

5. Criminal Code of Ukraine. *Bulletin of the Verkhovna Rada of Ukraine*. 2001. No. 25–26. Article 131

6. Kurakin O. M. The structure of the mechanism of legal regulation. *Scientific Bulletin of the Uzhhorod National University. Series: Law.* 2015. Issue 35. 546 p.

7. Manzhai O. V. Problems of regulatory and legal support of combating cybercrime in Ukraine. *Law forum.* 2017. No 1. P. 646–650.

8. Markov V. V. On the issue of foreign experience in countering cybercrime. *Law and Security.* 2017. No 2. 469 p.

9. Markov V. V. Statistical study of cybercrime indicators: methodological aspect. *Law and security.* 2018. No 2. 367 p.

10. Sen R. Yu. Experience of foreign countries in the field of cybercrime investigation Current issues of law enforcement agencies in the field of countering cybercrime. Kharkiv. 201 p.

11. Scams and Safety. Internet Fraud. URL: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud (in En.).

12. Warning, Advice and Reporting Point (WARP). URL: https://www.warpnetwork.org/services.html

N. Lugina, A. Bondarenko. Practical Aspects of Cybercrime Investigation – European Experience

The article examines the peculiarities of criminal offenses in the field of information and telecommunication technologies, and also draws attention to the main problems related to their detection, disclosure and investigation. Attention is focused on the rather large scale of the spread of cybercrime, not only in Ukraine, but also in the world community as a whole. The directions of international cooperation in the field of countering cybercrime, which in turn are based on international legal acts, are analyzed. Some experience of the struggle of European states, in particular the USA, Canada, France, Great Britain is taken into account. After all, one of the priority directions for improving the domestic legal system is the introduction of international ideas and concepts. In addition, the process of establishing a complete system of legal regulation of combating such a negative phenomenon as cybercrime is not possible without taking into account the achievements and gaps that were made by foreign countries during the formation of this institution. There is also an urgent need to study and implement the experience of foreign countries regarding the organization and effective functioning of units to combat cybercrime.

In the period of globalization, the rapid development of information technologies, new communication systems and computer networks is accompanied by the abuse of these technologies with criminal intentions. Therefore, it is equally important to be able to operate and understand what a concept such as "cyber security" represents. Cyber security primarily

refers to quick response to threats within the Internet. After all, the analysis of statistics shows that in most cases the objects of cyberattacks are the information resources of financial institutions, transport and energy supply companies, and state bodies that guarantee security, defense, and protection against emergency situations.

Keywords: *information, investigation of cybercrimes, European experience, combating cybercrime in the social dimension, legal mechanisms of interaction, global network, Convention on combating cybercrime.*

Стаття надійшла до редколегії 15 листопада 2022 року