УДК 343.9:004.49
DOI 10.33244/2617-4154.3(12).2023.211-218

А. С. Лупай,
здобувач першого (бакалаврського) рівня вищої освіти
e-mail: alinalupay2598@gmail.com
ORCID ID 0000-0001-6705-364X;
О. А. Павлюх,
канд. юрид. наук
e-mail: pavlyuh@gmail.com
ORCID ID 0000-0002-7850-8977;
А. І. Павлюх,
здобувач першого (бакалаврського) рівня вищої освіти,
Державний податковий університет
e-mail: pavlyuh@gmail.com
ORCID ID 0009-0006-3826-4310

АКТУАЛЬНІСТЬ ПИТАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ ЯК СКЛАДОВА ЗАГАЛЬНОКРИМІНАЛЬНОЇ ЗЛОЧИННОСТІ

У статті обґрунтовується існування у кримінальному праві поняття «кіберзлочинність», проводиться співвідношення понять «кіберзлочин» та «комп'ютерний злочин», сформульовано авторське поняття цих явищ, на основі аналізу спеціальної юридичної літератури наводиться авторська класифікація кіберзлочинів. У сучасних умовах інтенсивного розвитку інформаційного суспільства загальна кількість злочинів, пов'язаних з використанням комп'ютерної техніки та мережі «Інтернет», значно зростає, що дає підстави визначити актуальність появи самостійного шару в структурі загальнокримінальної злочини транснаціонального характеру – комп'ютерні злочини, оскільки злочини, пов'язані з інформаційними системами, загрожують організаціям, установам, особам і в цілому інформаційній безпеці України та інших країн. Термін «кіберзлочинність» у теорії наукового пізнання ще не знайшов свого остаточного визначення. Узагальненим терміном є розуміння кіберзлочинності як сукупності злочинних дій у кіберпросторі, ознакою яких буде їх вчинення за допомогою комп'ютерних систем (мереж), а також інших засобів доступу до кіберпростору та проти комп'ютерних систем, мережі. Класифікація кіберзлочинів відбувається за об'єктом та об'єктом втручання, способом його вчинення. Розвиток законодавчої бази та реагування на всі проблеми боротьби з кіберзлочинністю все ще відстає від розвитку інформаційних технологій. Механізми контролю за попередженням і розслідуванням правопорушень у кіберпросторі сьогодні

є обмеженими як соціально, так і технічно. Це зумовлює можливість стати жертвою використання інформаційних технологій у злочинних цілях завдяки автоматизованості та швидкості використання комп'ютера.

Ключові слова: *кіберзлочин, кіберзлочинність, комп'ютерний злочин, кібертехнології, кіберпростір.*

Постановка завдання. Метою статті є аналіз актуальності питання боротьби з кіберзлочинністю як складовою загальнокримінальної злочинності.

Постановка проблеми. Сьогодні кожен з нас не уявляє життя без інтернету. Спілкуємося в месенджерах, робимо покупки в інтернет-магазинах, замовляємо їжу, навіть за допомогою мобільного телефону керуємо побутовою технікою поза домом. Організації бізнес, ведуть бухгалтерський облік і подібні процедури за допомогою Всесвітньої павутини. Наш уряд також використовує так званий електронний уряд. Тому інтернет є скрізь, у всіх сферах нашого існування.

Це призвело до того, що багато злочинів як проти держави в цілому, так і проти окремих груп і навіть конкретних осіб вчиняються онлайн за допомогою комп'ютерів та інших пристроїв (гаджетів). Шахрайство та підробка, крадіжка особистих даних, витік особистих даних, хакерство, розсилка спаму, переслідування – це лише мала частина кіберпроблем, з якими багато хто з нас стикається щодня.

У світлі останніх подій проблема боротьби з кіберзлочинністю в Україні є надзвичайно актуальною.

Аналіз останніх досліджень і публікацій. Аспекти цієї теми досліджувалися такими авторами, як: П. Д. Біленчук, А. С. Білоусов, В. М. Бутузов, А. Ф. Волобуєв, В. Д. Гавловський, В. О. Голубєв, М. В. Гуцалюк, М. В. Карчевський, О. І. Котляревський, М. О. Кравцова, О. М. Лепеха, М. Ю. Літвінов, О. В. Манжай, А. І. Марущак, І. М. Осика, Л. П. Паламарчук, Д. В. Пашнєв, А. В. Реуцький та інші.

Об'єктом дослідження цієї статті є розгляд відповідальності за кіберзлочини за Кримінальним кодексом України (далі – КК України). Основним методом дослідження теми є теоретичний метод, який застосовується для аналізу статтей КК України у сфері вирішення сучасних проблем у боротьбі з кіберзлочинами.

Виклад основного матеріалу. Боротьба з кіберзлочинністю неможлива без глибокого розуміння та правових проблем регулювання інформаційних мереж. Саме аналіз взаємозв'язку між технічними характеристиками мережі та зумовленими цими характеристиками правовими і соціальними складнощами, з якими стикаються законодавці та правоохоронні органи, є першим кроком до можливого вироблення механізмів адекватного реагування на розвиток і зростання кіберзлочинності.

Відсутність механізмів контролю. Основна проблема боротьби зі злочинністю у мережі «Інтернет» полягає у транснаціональності самої мережі та у відсутності механізмів контролю, необхідних для правозастосування. Коли мережа «Інтернет» створювалася технологічно як структура без ієрархії і без якогось «ядра», зруйнувавши які, можна було б паралізувати її роботу, навряд чи хтось міг уявити масштаби розвитку проєкту, що спочатку не призначений для широкої аудиторії [1, с. 718].

Основною метою створення цієї мережі була стійкість до атак ззовні, і навряд чи хтось міг передбачити подальший масштаб її розвитку та її соціальну і економічну роль у майбутньому. Саме відсутність розроблених механізмів контролю мережі зсередини разом з її доступністю та легкістю використання стала однією з глобальних проблем інформаційної спільноти [1]: децентралізована структура мережі та відсутність національних кордонів у кіберпросторі зумовили можливості для зростання злочинності та на роки відклали розробку механізмів соціального та правового контролю у сфері використання інформаційних мереж для скоєння злочинів.

В останні роки інформаційні мережі розвиваються досить швидко, щоб існуючі механізми контролю встигали реагувати на нові проблеми. Хмарна обробка даних, автоматизація атак, уразливість персональної інформації в соціальних мережах: поширення так званої «інформаційної зброї», прикладом якої є вірус Stuxnet, розроблений, на думку фахівців, для атак на ядерну промисловість Ірану, але при цьому завдав чималої шкоди інфраструктурі багатьох інших країн – на всі ці проблеми правове регулювання поки що не може знайти адекватної відповіді.

Загалом кіберзлочини – це умисні злочини, які виражаються у вигляді незаконних дій (бездіяльностей), скоєні з використанням кібертехнологій у віртуальному середовищі (кіберпростір) із застосуванням телекомунікаційних засобів та засобів, зокрема мережі «Інтернет», які є злочинними знаряддями чи предметами протиправних посягань.

Під кіберпростором розуміються інформаційно-телекомунікаційні мережі, комп'ютерні локальні мережі, глобальна мережа «Інтернет». Кіберпростір є доступним для кожного інформаційного користувача, що дозволяє злочинцеві, перебуваючи на території однієї держави, вчинити злочин щодо іноземних громадян, тим самим злочин має транснаціональний характер.

Кібертехнології – технічні засоби (персональні комп'ютери, ноутбуки, смартфони) та сама інформація і її носії.

Вперше на міжнародному рівні посилання на кіберзлочинність було використано в Конвенції про кіберзлочинність 2001 року, але вона не дає визначення цьому поняттю. Закон України «Про основні засади забезпечення кібербезпеки України» визначає кіберзлочин як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України. Крім того, закон ототожнює кіберзлочин з комп'ютерним злочином [2].

Разом з тим С. Буяджи зауважує та визначає кіберзлочинність як сукупність окреслених кримінальним законом вчинків, скоєних на певній території, або щодо об'єктів, розташованих на ній, за відповідний період, вчинених у віртуальному просторі шляхом деструктивного впливу на комп'ютерні системи, комп'ютерні мережі й комп'ютерні дані [1, с. 45].

Узагальненим терміном є розуміння кіберзлочинності як сукупності злочинних дій у кіберпросторі, ознакою яких буде їх вчинення за допомогою комп'ютерних систем (мереж), а також інших засобів доступу до кіберпростору та проти комп'ютерних

систем. Тому сама класифікація кіберзлочинів відбувається за об'єктом та об'єктом втручання, способом його вчинення.

Залежно від типу загроз кібербезпеку можна розглядати як забезпечення стану захищеності особи, суспільства, держави від впливу неякісної інформації, інформації та джерел інформації від непропорційного впливу третіх осіб, права на інформацію і свободу людини і громадянина.

З огляду на функції кіберполіції, як новоствореного 5 листопада 2015 року структурного підрозділу Національної поліції України, класифікація кіберзлочинів має таку структуру:

1. У сфері використання платіжних систем:

скімінг (шимінг) – незаконне копіювання вмісту слідів магнітної смуги (чіпів) банківських карток;

навчання готівці – викрадення готівки з банкомату шляхом встановлення спеціальної утримуючої накладки на намет банкомату;

кардінг – незаконні фінансові операції, що здійснюються за допомогою платіжної картки або її даних, які не ініціюються та не підтверджуються її держателем;

несанкціоноване зняття коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування.

2. У сфері електронної комерції та господарської діяльності:

фішинг – виманювання у користувачів інтернету їхніх даних для входу та паролів до електронних гаманців, сервісів онлайн-аукціонів, грошових переказів чи обміну валюти тощо;

онлайн-шахрайство – конфіскація коштів громадян через інтернет-аукціони, інтернет-магазини, вебсайти та засоби зв'язку.

3. У сфері інтелектуальної власності:

піратство – незаконне розповсюдження інтелектуальної власності в інтернеті;

кардшерінг – надання незаконного доступу до супутникового та кабельного спостереження.

4. У сфері інформаційної безпеки:

соціальна інженерія – технологія управління людьми в інтернет-просторі;

шкідливе програмне забезпечення – створення та розповсюдження вірусів і шкідливого програмного забезпечення;

незаконний контент – контент, що пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості та насильства;

рефайлінг – незаконна заміна телефонного трафіку.

Транснаціональний характер мережі «Інтернет» і відсутність необхідних для правоохоронної діяльності механізмів контролю над інформаційними мережами.

Ця проблема виникає через децентралізовану структуру інформаційної мережі та відсутність національних кордонів у кіберпросторі.

В. Б. Боровиків комп'ютерні кримінальні правопорушення визначає як навмисні суспільно небезпечні діяння, які заподіюють шкоду або створюють загрозу заподіяння

шкоди суспільним відносинам, що регулює безпечне виробництво, зберігання, використання або поширення інформації або інформаційних ресурсів [3].

Водночас у чинному Кримінальному кодексі України є «спеціалізований» розділ, який визначає відповідальність за кіберзлочини – розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж та мереж електрозв'язку», що складається із 6 статей.

Кіберпереслідування (кібersталкінг) – це відносно нове явище, саме тому досі немає єдиного визначення цього поняття, яке було прийнятне і для правоохоронних органів, і для засобів масової інформації. Тому насамперед варто ознайомитися з найчастіше вживаними термінами.

Так, кібersталкінг, згідно з Оксфордським словником, – це повторюване використання електронних пристроїв зв'язку для переслідування або залякування когось, наприклад, шляхом надсилання листів з погрозами електронною поштою.

Основним законом держави є Конституція. Так, її стаття 32 прямо вказує на те, що втручання у особисте та сімейне життя людини заборонено. Виняток становлять законодавчо передбачені випадки і лише з урахуванням інтересів національної безпеки, прав людини та економічного добробуту [4].

Однією з проблем є удосконалення кодифікації кіберзлочинності в кримінальному праві України.

Дослідження провідних науковців у галузі комп'ютерної злочинності та комп'ютерної безпеки, а саме: П. Д. Біленчука, А. В. Геллера, Р. А. Калюжного, М. В. Карчевського, А. М. Супруженка, Д. Чиркова. К. та ін. доведено, що терміни «комп'ютерна злочинність», «кіберзлочинність» у загальному розумінні можуть бути ефективно використані у процесі дослідження кримінологічних, кримінально-процесуальних, криміналістичних аспектів.

З погляду національної кримінально-правової дискусії найбільш прийнятним варто вважати визначення кіберзлочинності як «злочинів із використанням інформаційних технологій».

Так, у розділі XVI Особливої частини КК України міститься перелік кримінальних правопорушень у сфері використання електронно-обчислювальних машин, систем і комп'ютерних мереж та мереж електронного зв'язку, який зазначений у стст. 361, 361-1, 361-2, 362, 363, 363-1.

Крім того, в окремих дослідженнях (О. В. Орлов, Ю. М. Оніщенко) розглядається розширення переліку так званих «старих злочинів» кіберзлочинів, на які поширюється дія Конвенції про кіберзлочинність [5, с. 7]. Ці дії передбачають:

— різні види підробок (стст. 199, 200, 215, 216, 224, 290, 318, 358, 366 КК України);

— шахрайство з різними предметами (стст. 190, 192, 222, 262, 308, 312, 313, 357, 410 КК України);

— ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301 КК України);

— порушення авторського права й суміжних справ (ст. 176 КК України).

Статтю 182 Кримінального кодексу України присвячено порушенням недоторканності приватного життя людини. Так, згідно з її пунктом 1, для того, хто нелегально збирає, зберігає, використовує, видаляє, поширює конфіденційну інформацію про інших осіб, передбачено такі види покарання як штраф (500–1 000 неоподатковуваних мінімумів доходів громадян), виправні роботи (від 2-х років), арешт (до півроку) або обмеження свободи (до 3-х років). У разі повторного правопорушенні штраф не передбачено, але можливі арешт, обмеження або позбавлення волі [6].

Предмет кримінального правопорушення у цьому випадку – конфіденційна інформація про суб'єкта, тобто дані про приватне життя людини, а саме про його сімейний стан, релігійну приналежність, майновий стан та освіту, його стан здоров'я, а також дату та місце появи на світ, інші відомості. Згідно з коментарем до КК України у приватне життя становить сферу життєдіяльності окремо взятої особи, зокрема його з іншими людьми, приватні активності, стосунки в сім'ї – усе, що стосується його способу життя. Водночас інформація, яку раніше опублікували у засобах масової інформації чи іншим способом, не вважається, згідно з нашим законодавством, конфіденційною [7].

Кіберсталкерів, які порушують ваші права, також можна було б спробувати залучити до відповідальності за наклеп, якби не проблема її декриміналізації. Так, до 2001 року, доки діяв КК України 1960 року, за поширення неправдивих домислів, що ганьблять честь іншої людини, було передбачено кримінальну відповідальність. Але КК України 2001 року виключив зі свого змісту це питання на підставі визнання наклепу особистим немайновим правовим порушенням, яке стосується ведення цивільно-правової сфери.

Висновки. Підсумовуючи вищевикладене зазначимо, що кіберзлочини на підставі представленого поняття можна розглянути у вузькому та широкому значенні.

Кіберзлочин у вузькому розумінні – це будь-яке протиправне діяння, яке здійснюється шляхом проведення електронних операцій, метою якого є отримання доступу до комп'ютерних систем та інформаційних даних.

Кіберзлочин у широкому розумінні – це будь-який злочин, скоєний у комп'ютерній системі або глобальній мережі, що складається з незаконного зберігання, розповсюдження електронної інформації.

Потрібно зазначити, що до визначення кіберзлочинності включається також протиправне втручання в комп'ютерні засоби, програми та мережі, несанкціонована модифікація комп'ютерних відомостей, інші протиправні дії, вчинені з використанням комп'ютерів, комп'ютерних мереж та програм.

Однак, оскільки жодна держава не може захистити себе, вживаючи заходів лише на національному рівні, для комплексної протидії кіберзлочинності потрібні:

– гармонізація кримінального законодавства про кіберзлочини на міжнародному рівні;

– розробка на міжнародному рівні та імплементація до національного законодавства процесуальних стандартів, що дозволяють ефективно розслідувати злочини у глобальних інформаційних мережах, отримувати, досліджувати та подавати електронні докази з урахуванням транскордонності проблеми;

– налагоджена співпраця правоохоронних органів під час розслідування кіберзлочинів на оперативному рівні;

– механізм вирішення юрисдикційних питань у кіберпросторі.

Отже, міжнародне співробітництво є ключовим моментом у ліквідації правового вакууму, що існує між розвитком інформаційних технологій та реагуванням на них законодавства. Процес вироблення заходів на міжнародному рівні, як показує досвід, сам собою є комплексною проблемою. Однак це єдиний шлях забезпечити безпеку користувачів і держави від електронних посягань, а також ефективно розслідувати та переслідувати кіберзлочини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Буяджи С. А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект : дис. ... канд. юрид. наук. 12.00.01. Київ, 2018. 203 с.

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL : http://surl.li/ajfjh (дата звернення: 20.03.2023).

3. Боровиків В. Б. Кримінальне право. 2015. URL : https://stud.com.ua/53995/pravo/kriminalne_pravo (дата звернення: 20.03.2023).

4. Конституція України від 28 чер. 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.

5. Актуальні напрями державної політики України у сфері боротьби з кіберзлочинністю. *Теорія та практика державного управління.* 2013. Вип. 3. С. 3–9. URL : http://gov.ua/j-pdf/Tpdu_2013_3_3.pdf (дата звернення: 20.03.2023).

6. Кримінальний кодекс України від 5 квіт. 2001 р. № 2341-III. *Відомості Верховної Ради України.* 2001. № 25–26. Ст. 131.

7. Коментар до статті 182. Порушення недоторканності приватного життя. Коментар до Кримінального кодексу. *Юридичні послуги Online.* 2020. URL : http://yurist-online.com/ukr/uslugi/yuristam/kodeks/024/179.php (дата звернення: 20.03.2023).

8. Шевченко А. Є., Павлюх О. А., Санжаров В. А. Питання кібербезпеки в сучасному італійському законодавстві: національний безпековий периметр. *Наукові тренди постіндустріального суспільства* : матеріали IV Міжнародної наукової конференції, м. Суми, 31 березня 2023 р. Вінниця : Європейська наукова платформа, 2023. С. 80–82.

REFERENCES

1. Buyadzhi S. A. Legal regulation of the fight against cybercrime: theoretical and legal aspect : PhD. 12.00.01. Kyiv, 2018. 203 c.

2. On the basic principles of ensuring cybersecurity of Ukraine : Law of Ukraine of. 05.10.2017 № 2163-VIII. URL : http://surl.li/ajfjh (accessed March 20, 2023).

3. Borovykiv V. B. Criminal law. 2015 p. URL : https://stud.com.ua/53995/pravo/kriminalne_pravo (accessed March 20, 2023).

4. Constitution of Ukraine of June 28, 1996 No. 254к/96-ВР. *Bulletin of the Verkhovna Rada of Ukraine.* 1996. № 30. Art. 141.

5. Actual directions of state policy of Ukraine in the field of combating cybercrime. *Theory and practice of public administration.* 2013. Issue 3. C. 3–9. URL : http://gov.ua/j-pdf/Tpdu_2013_3_3.pdf (accessed March 20, 2023).

6. Criminal Code of Ukraine of April 05, 2001. No. 2341-III. *Bulletin of the Verkhovna Rada of Ukraine.* 2001. № 25–26. Art. 131.

7. Commentary to Article 182. Violation of privacy. Commentary to the *Criminal Code Legal Services Online.* 2020. URL : http://yurist-online.com/ukr/uslugi/yuristam/kodeks/024/179.php (accessed March 20, 2023).

8. Shevchenko A. E., Pavliukh O. A., Sanzharov V. A. Cybersecurity issues in modern Italian legislation: national security perimeter. *Scientific trends of the post-industrial society* : materials of the IV International Scientific Conference, Sumy, March 31, 2023. European Scientific Platform, 2023. C. 80–82.

A. Lupai, O. Pavliukh, A. Pavliukh. The Relevance of the Issue of Combating Cybercrime as a Component of General Criminal Activity

The article substantiates the existence of the concept of "cybercrime" in criminal law, and also draws a correlation between the concepts of "cybercrime" and "computer crime", and formulates the author's own concept of these phenomena, and based on the analysis of special legal literature, the author provides the author's classification of cybercrime. In today's conditions of intensive development of the information society, the total number of crimes related to the use of computer equipment and the Internet is growing significantly, and this gives rise to the relevance of the emergence of an independent layer in the structure of transnational crime – computer crime, since crimes related to information systems threaten organizations, institutions, individuals and, in general, the information security of Ukraine and other countries. The term "cybercrime" has not yet found its final definition in the theory of scientific knowledge. A generalized term is the understanding of cybercrime as a set of criminal acts in cyberspace, which will be characterized by their commission with the help of computer systems (networks), as well as other means of access to cyberspace and against computer systems and networks. Cybercrime is classified by the object and target of interference and the method of its commission. The development of the legislative framework and response to all the problems of combating cybercrime still lags behind the development of information technology. Mechanisms for controlling the prevention and investigation of offenses in cyberspace are currently very limited both socially and technically. This leads to the possibility of becoming a victim of the use of information technology for criminal purposes due to the automation and speed of computer use.

Keywords: *cybercrime, cybercrime, computer crime, cybertechnology, cyberspace.*

Стаття надійшла до редколегії 20 квітня 2023 року