УДК 344.65

О. Довженко,
аспірант кафедри кримінального процесу
Одеського державного університету внутрішніх справ

ПОНЯТТЯ КІБЕРЗЛОЧИНУ З КРИМІНАЛІСТИЧНОЇ ПОЗИЦІЇ

Поняття кіберзлочинів та кіберзлочинності широко використовуються в сучасній літературі у зв'язку з науково-технічним розвитком у XXI столітті. Кібернетичні технології стали невід'ємною частиною всіх сфер життєдіяльності людини. Зокрема, за допомогою цифрових систем дистанційного банківського обслуговування та за каналами зв'язку за допомогою електронних засобів та електронних носіїв інформації, технічних пристроїв та комп'ютерних програм здійснюється переказ чималих грошових коштів.

За даними Організації Об'єднаних Націй, у світі більше двох мільярдів осіб мають доступ до мережі «Інтернет» [8]. Зі збільшенням кількості її користувачів збільшується і кількість осіб, що здійснюють Глобальну мережу для здійснення протиправних діянь. Комп'ютерні та телекомунікаційні системи відкривають не тільки унікальні можливості для задоволення найбільш широких запитів людини в усіх сферах її життєдіяльності та функціонування держави, але й створюють сприятливі умови для різноманітних злочинних дій. З'являються цілі організовані групи, що створюють злочинний бізнес, який ґрунтується на шахрайстві у сфері високих технологій, за допомогою якого отримуються колосальні прибутки.

Злочини, що здійснюються за допомогою комп'ютерних технологій та мережі «Інтернет», слід виділити в окрему категорію – кіберзлочини, тобто такі злочини, що скоєні за допомогою цифрових технологій. Найбільш поширеними з таких злочинів є:

– шахрайство за допомогою систем дистанційного банківського обслуговування через викрадення та незаконне використання автентичних даних, таких як паролі, криптографічні ключі, одноразові паролі та ін., із метою незаконного списання грошей з рахунків фізичних та юридичних осіб;

– атаки проти зареєстрованих брендів та торгівельних марок шляхом створення так званих фішингових доменів, створення Інтернет-ресурсів, які компрометують бренд чи займаються шахрайством від його імені. Подібні атаки фіксувалися проти найбільших брендів, зокрема проти google;

– атаки проти захисних механізмів систем дистанційного банківського обслуговування (DDoS-атаки), які слугують прикриттям для проникнення в систему чи створюють незручності для клієнтів як засіб недобросовісної конкурентної боротьби;

– внутрішнє шахрайство з використанням комп'ютерних технологій, наприклад, підміна платіжних документів та фінансової інформації, викрадення масивів даних, компрометація конфіденційності інформації.

Найбільш поширеним способом злочинних дій слід визнати шахрайство в системах дистанційного обслуговування. Цілі групи кіберзлочинців займаються організованим викраденням ключів для систем ДБО з метою подальшого отримання готівкових грошових коштів. Частіше за все, такі дії здійснюються за допомогою шкідливого програмного забезпечення через мережу «Інтернет». Таке шкідливе програмне забезпечення містить певний код,

який вбудовується до програмного забезпечення комп'ютера, що піддається атаці, винаходить, що цей комп'ютер використовується для роботи з системою ДБО, та здійснює копіювання ключів (логіну та паролю) користувача, а потім передає інформацію зловмисникам. Крім того, можливі випадки, коли переказ грошових коштів здійснюється безпосередньо з комп'ютера жертви через програмне забезпечення для адміністрування, також встановленого зловмисниками через мережу «Інтернет». Із розвитком інформаційних технологій цей та інші подібні кіберзлочини стають однією з найбільших проблем не тільки для окремих держав, а й для міжнародної спільноти в цілому.

До цього моменту ані в міжнародних документах [3; 8], ані в національному законодавстві України не розроблена єдина термінологія та єдиний підхід до виявлення та поняття кіберзлочинності, що застосовується поряд із такими поняттями, як комп'ютерна злочинність, злочини в телекомунікаційних системах, злочини у сфері високих технологій, інформаційні злочини, злочини у сфері комп'ютерної безпеки, злочини у сфері комп'ютерної інформації тощо.

Однак поняття «кіберзлочинність» (в англомовному варіанті – cybercrime) семантично ширше, ніж «комп'ютерна злочинність» (computercrime), і більш точно відображає природу такого глобального явища, як злочинність в інформаційному просторі. Якщо термін «кіберзлочинність» співвідноситься як із використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж, то поняття «комп'ютерна злочинність» в основному стосується злочинів, що здійснюються проти електронних пристроїв і даних, що на них зберігаються.

В опублікованих теоретичних джерелах тривають дискусії про підходи до визначення поняття «кіберзлочини». По суті питання висловлюються в основному кримінологи [1] або фахівці в галузі кримінального права [7]. Відсутність повноцінного, вивіреного термінологічного апарату, що забезпечує сферу розглянутих злочинів, зайвий раз підкреслює відсутність повного розуміння суті даної проблеми, її актуальність і стурбованість як із боку наукового співтовариства, так і з боку громадянського суспільства, новими погрозами зростаючих масштабів злочинності.

Існуюче різноманіття визначень можна звести до декількох основних підходів. Відповідно до першого кіберзлочином є будь-яке протиправне діяння, що скоєно за допомогою чи у зв'язку з комп'ютерними пристроями, зокрема, такі злочини, як незаконне зберігання чи розповсюдження інформації шляхом використання комп'ютерних технологій. У цілому кіберзлочини пов'язуються з різноманітними правопорушеннями, які здійснюються в електронних мережах.

Другий підхід полягає у віднесенні до кіберзлочинів протиправних діянь, що здійснюються за допомогою комп'ютерного та мобільного зв'язку в інформаційних мережах, у першу чергу – в мережі Інтернет, а також за допомогою їхніх програмних компонентів відносно інформації, що розміщується у віртуальному просторі мережі «Інтернет». Цей підхід можна назвати вузьким та таким, що концентрується виключно на злочинах в електронних мережах.

Можна виділити також інтеграційний підхід, який намагається об'єднати два вищевказаних підходи. Відповідно до нього кіберзлочинами є суспільно небезпечні діяння, що скоюються за допомогою засобів та способів комп'ютерного та мобільного зв'язку, в яких електронний пристрій є знаряддям чи предметом кримінальних посягань у віртуальному просторі. Із точки зору кримінального права, таким чином, кіберзлочином є винно скоєне суспільно небезпечне та кримінально карне втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, скоєні

за допомогою чи через комп'ютери, комп'ютерні мережі та програми, а також за допомогою чи через інші пристрої доступу до інформаційного (віртуального) простору.

До визначення подібних злочинів саме як «кіберзлочинів» (а не, наприклад, «комп'ютерних злочинів») підштовхує термінологія, яка міститься в чинних міжнародних договорах України. Зокрема, саме цей термін використано в Конвенції Ради Європи про кіберзлочинність, що набрала чинності для України 1 липня 2006 року [3]. Нею до кіберзлочинів було віднесено незаконний доступ до комп'ютерних систем (ст. 2), нелегальне перехоплення даних, що передаються цифровими каналами зв'язку (ст. 3), втручання в дані, що зберігаються в комп'ютерних системах чи передаються електронними каналами зв'язку (ст. 4), втручання в комп'ютерні системи (ст. 5), зловживання комп'ютерними пристроями (ст. 6), підробки, пов'язані з комп'ютерами (ст. 7), шахрайство, пов'язане з комп'ютерами (ст. 8), правопорушення, пов'язані з дитячою порнографією (ст. 9), правопорушення, пов'язанні з порушенням авторських чи суміжних прав (ст. 10).

У Конвенції передбачено лише невелика частина злочинів у сфері комп'ютерної інформації. Левова частка кіберзлочинності залишається за рамками статистики. Якщо говорити точніше, то в офіційну статистику потрапляє лише 10%, у кращому випадку – 12% від вчинених злочинних діянь [5].

Спроба пояснення сутності поняття кіберзлочинності була зроблена Конгресом ООН із попередження злочинності та поводження з правопорушниками. Згідно з його резолюцією «кіберзлочин – це будь-який злочин, який може відбуватися за допомогою комп'ютерної системи або мережі, в рамках комп'ютерної системи або мережі або проти комп'ютерної системи або мережі». Іншими словами, до кіберзлочинів може бути віднесено будь-яке протиправне діяння, вчинене в електронному середовищі [2].

У 2013 році Управлінням ООН із боротьби з наркозлочинністю був опублікований звіт «Усебічне дослідження проблеми кіберзлочинності та заходи у відповідь із боку держав-членів, міжнародної спільноти та приватного сектора», в якому поняття «кіберзлочинність» було поставлено в залежність від контексту і мети вживання цього терміну. Крім того, як підкреслюється у звіті, в перелік комп'ютерних злочинів включені не тільки злочини проти конфіденційності, цілісності і доступності даних, але і будь-які дії, спрямовані на протизаконне одержання прибутку, контент-злочини та інші протиправні діяння в кіберпросторі. При цьому, як відзначають автори звіту, «у створенні якогось універсального визначення кіберзлочинності немає необхідності, адже, наприклад, у цілях міжнародного співробітництва в розслідуванні злочинів набагато важливіше гармонізувати норми, які стосуються збору і надання електронних доказів. Ця необхідність не обмежується якимось штучним терміном «кіберзлочини», оскільки на електронних носіях і в електронних комунікаціях може міститися інформація, що належить до будь-якого виду злочинів, скоєних як у кіберпросторі, так і поза ним» [8].

Значно ширше розглядають комп'ютерні злочини автори «Модельного закону» про кіберзлочинність Міжнародного союзу електрозв'язку (2009 г.), співвідносячи їх із протиправними діяннями, вчиненими в кіберпросторі, і предметом атак яких є: «комп'ютери, комп'ютерні системи, мережі, їх комп'ютерні програми, комп'ютерні дані, дані контенту, рух даних і користувачі» [9].

Розслідування злочинів, скоєних у кіберпросторі, вимагає як технічних, так і теоретичних знань. З урахуванням гострого дефіциту останніх виникає необхідність обґрунтування єдиного поняття кіберпростору з точки зору криміналістики, що сприятиме поглибленню і розширенню термінології теоретичної бази комп'ютерної криміналістики. Кіберпростір (від кібернетика

і простір) – метафорична абстракція, яка використовується в філософії і в комп'ютерній технології, віртуальна реальність, що представляє ноосферу, другий світ як «усередині» комп'ютерів, так і комп'ютерних мереж. Поняття кіберпростору сьогодні використовується під час опису об'єктів, широко поширених у комп'ютерній мережі. Наприклад, веб-сайт може бути метафорично описаний як «такий, що знаходиться в кіберпросторі». Допускаючи подібну інтерпретацію, можна говорити про інтернет-події, що відбуваються не в країнах або містах, де фізично знаходяться сервери або учасники, а в кіберпросторі. Прикладаючи поняття кіберпростору до поняття злочину, слід говорити про кіберзлочини як такі злочини, що відбуваються в кіберпросторі.

Разом із тим відсутність наукового обґрунтування і чітко визначеного понятійного апарату в даній сфері не сприяє правильній кваліфікації кіберзлочинів та їх якісному розслідуванню. Безумовно важливим є і юридичне закріплення термінології і сформульованої дефініції кіберпростору, що необхідно для регламентації слідчих дій під час встановлення обстановки скоєння злочину.

Пізнаючи кіберпростір із позицій криміналістики, відзначимо найважливішу методологічну специфіку цієї науки: вона досліджує будь-які предмети матеріального і ідеального макро- і мікросвіту. Іншими словами, склад розв'язуваних задач під час дослідженні кіберпростору і кіберзлочинів зумовлений нескінченним різноманітністю слідчо-судових і експертних ситуацій, у силу чого методологічний потенціал вивчення віртуальної злочинності з обов'язковою необхідністю повинен втілити в собі все багатство загальнонаукового і спеціального криміналістичного знання.

У контексті сказаного можливим представляється констатувати: застосування системного підходу для вирішення важливого завдання, пов'язаного з підвищенням ефективності виявлення та розслідування кіберзлочинів, зумовило необхідність створення класифікації кіберпростору і кіберзлочинів, що вимагає встановлення їх механізмів і закономірностей, обґрунтування ієрархії внутрішніх і зовнішніх, прямих і зворотних зв'язків. При цьому дослідження зазначених понять бачиться як синтетичне цілісне утворення, в якому воєдино пов'язані його різні сторони, що визначає його актуальність і практичну спрямованість і є умовою вдосконалення методики розслідування інциденту, що має ознаки злочину в кіберпросторі.

Очевидно, що така робота далека від завершення навіть у науковій літературі, не кажучи вже про законодавчу техніку. Проте вона має проводитися із чітким усвідомленням кінцевої мети – розроблення концепції та стрункого законодавчого визначення кіберзлочину як злочину, що скоюється в кіберпросторі.

Ключові слова: кіберзлочин, комп'ютерний злочин, злочин у кіберпросторі, розслідування кіберзлочинності, розслідування комп'ютерних злочинів.

Стаття присвячена дослідженню кіберзлочинів із точки зору криміналістики. Розглядаються різні підходи до визначення цього поняття. Доводиться, що для позначення відповідної категорії злочинів слід використовувати саме термін «кіберзлочини». Розглядається кіберпростір як середовище, в якому скоюються кіберзлочини.

Статья посвящена изучению киберпреступлений с точки зрения криминалистики. Рассматриваются разные подходы к определению этого понятия. Доказывается, что для обозначения соответствующей категории преступлений следует использовать именно термин «киберпреступление». Рассматривается киберпространство как среда, в которой совершаются киберпреступления.

The article deals with cybercrime from the point of view of criminalistics. It analyzes various approaches towards the definition of this notion. It is proven that this category of crimes should be regarded exactly as cybercrimes. It further reviews the cyberspace as a space where cybercrimes are committed.

Література

1. Гвоздецька М. О. Кримінологічна характеристика кіберзлочинності: сучасний стан, структура та специфіка вивчення. Матеріали всеукраїнської науково-практичної конференції, м. Кропивницький, 23-25 листопада 2016 р. С. 52–53.

2. Десятый конгресс Организации Объединённых Наций по предупреждению преступности и обращению с правонарушителями. Вена. 10-17 апреля 2000. URL : https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-RU.pdf.

3. Конвенція Ради Європи про кіберзлочинність. URL : http://zakon.rada.gov.ua/laws/show/994_575.

4. Конвенція Ради Європи про кіберзлочинність. URL : http://zakon.rada.gov.ua/laws/show/994_575.

5. Номоконов В.А. Киберпреступность: прогнозы и проблемы борьбы. Криминология: вчера, сегодня, завтра. 2012. № 24. С. 152–153.

6. Окинавская хартия глобального информационного общества (Окинава, 22 июля 2000 года). URL : http://zakon.rada.gov.ua/laws/show/998_163.

7. Римарчук Г.С. Юридична природа кіберзлочинів. Науковий вісник Ужгородського національного університету. Серія ПРАВО. Вип. 24. Т. 4. С. 54–57.

8. Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. URL : https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf.

9. ITU Model Cybercrime Legislation: Project Overview. URL : http://www.itu.int/ITU-D/cyb/cybersecurity/docs/model-cybercrime-law-project-overview.pdf.