УДК 343.3 /.7

Піцик Ю. М.,
начальник відділу роботи з кадрами
прокуратури міста Києва

ДО ВИЗНАЧЕННЯ ПОНЯТТЯ КІБЕРЗЛОЧИНІВ ПРОТИ ВЛАСНОСТІ

TO DETERMINATION OF THE CONCEPT OF COBERSOLVINS AGAINST PROPERTY

У статті розглянуто проблеми визначення поняття «кіберзлочини проти власності» у національному законодавстві. З цією метою проаналізовано нормативно-правові акти України та наукові позиції вчених.

Ключові слова: *кіберзлочини, кіберзлочини проти власності, злочини у сфері інформаційних відносин, кіберзлочинність, комп'ютерні злочини.*

В статье рассмотрены проблемы определения понятия «киберпреступлений против собственности» в национальном законодательстве. С этой целью проанализированы нормативно-правовые акты Украины и научные позиции ученых.

Ключевые слова: *киберпреступления, киберпреступления против собственности, преступления в сфере информационных отношений, киберпреступность, компьютерные преступления.*

The article deals with the problems of definition of the concept of «cybercrime against property» in the national legislation. To this end, the normative legal acts of Ukraine and scientific positions of scientists are analyzed.

Key words: *cybercrime, cybercrime against property, crimes in the field of information relations, cybercrime, computer crimes.*

Постановка проблеми. У всіх державах світу, а Україна не є виключенням, динамічно розвиваються нові сфери суспільного життя, що ґрунтуються передусім на використанні сучасних інформаційних технологій, локальних та глобальних комп'ютерних мереж, зокрема Інтернету. Відповідні темпи розвитку українського сегменту Всесвітньої павутини сьогодні випереджають загальносвітові. Так, за даними міжнародних організацій, у 2015 році Україна увійшла до першої десятки держав Європи за кількістю інтернет-користувачів – доступ до Світової мережі мають близько 22 млн українців, що становить 59% населення [1].

Можливості, надані комп'ютерними технологіями, знайшли широке застосування при вчиненні багатьох злочинів, у тому числі проти власності, а саме: шахрайств (у тому числі найбільш поширених їх видів – шахрайських дій з кредитними картками); несанкціонованих втручань у роботу електронно-обчислювальних машин з метою викрадення інформації, яка на них зберігається; вимагань, які вчиняються за допомогою доступу в Інтернет тощо. Однак, незважаючи на наявність низки чинних нормативно-правових актів, вітчизняне законодавство не містить чітко визначених понять, які є відправними у сфері протидії злочинності, зокрема, таких, як «кіберзлочини» та «кіберзлочини проти власності».

Аналіз останніх досліджень і публікацій. Питанням нормативно-правового визначення основних термінів у сфері інформаційної безпеки приділялася увага у наукових працях Е. Авер'янової, Д. Азарова, В. Болгова, С. Бородіна, В. Бутузова, В. Вєхова, Н. Гадіон, О. Гладуна, В. Голубєва, А. В. О. Книженко, О. Користіна, Л. Краснова, М. Карчевського, М. Литвинова, Ю. Ляпунова, С. Максимова, А. Музики, А. Новікова, П. Смагіна, М. Погорецького, В. Шеломенцева та інших. Однак не дослідженими лишились питання, пов'язані з проблемами визначення у національному законодавстві поняття «кіберзлочинів проти власності».

Метою статті є з'ясування проблемних питань, які виникають при визначенні поняття «кіберзлочини проти власності».

Виклад основного матеріалу дослідження. У зарубіжних країнах, таких як США, Німеччина, Швейцарія, «комп'ютерна злочинність» (*computer crime*) має правове визначення та закріплення як кримінально-правове поняття. У США при визначенні цієї категорії правопорушень у законодавстві вживається термін «кіберзлочинність» (*cyber crime*). Однак прокурор прокуратури Сан-Франциско Дель Росаріо Конрад, який очолює структурний підрозділ з розкриття та розслідування злочинів у вказаній сфері, пропонує вживати більш широке поняття «злочини у сфері високих (новітніх) технологій», оскільки сфера його діяльності поширюється і на загальнокримінальні злочини, які вчинені з використанням технологічних інновацій [2].

Відправною точкою для визначення поняття «кіберзлочин» є Конвенція про кіберзлочинність від 23 листопада 2001 року (далі – Конвенція). Сьогодні вона ратифікована 18 державами та підписана 25 країнами, у тому числі й Україною (7 вересня 2005 року) [3]. Згодом, нашою державою було ратифіковано додатковий протокол до Конвенції, що стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (Додатковий протокол) [4]. Проте, терміни, які вживаються в Конвенції та додатковому протоколі до неї, так і не знайшли свого закріплення у вітчизняному законодавстві. Крім того доцільно вказати, що ані у тексті Конвенції, ані у тексті

Додаткового протоколу до неї не міститься визначення поняття кіберзлочину та суміжних з ним понять, утім наявний перелік діянь, за які на національному рівні пропонується встановити кримінальну відповідальність, та наводиться їх умовна класифікація залежно від об'єкта правовідносин.

Чинне українське законодавство до сьогодні не містить визначеного поняття як «кіберзлочин» та «кіберзлочин проти власності». Зокрема чинним Кримінальним кодексом України (далі – КК України) передбачено кримінальну відповідальність за: 1) несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361); 2) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1); 3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2); 4) несанкціоновані дії з інформацією, яка оброблюється в електронно- обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362); 5) порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363); 6) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1). А щодо кіберзлочинів проти власності взагалі чинний КК України передбачає відповідальність лише за злочин, передбачений ч. 3. ст. 190 КК України. Тому вітчизняне законодавство лише частково задовольняє потреби сьогодення, оскільки не містить визначення понять, які є відправними у сфері формування державної інфраструктури інформаційної безпеки та вичерпного переліку злочинів у цій сфері.

Чинним КК України охоплено лише частину відповідних кримінально караних діянь, для позначення яких, ґрунтуючись на аналізі сутності та ознак посягань, використовують такі термінологічні звороти, як «кіберзлочини», «злочини у сфері ІТ-технологій», «високотехнологічні злочини», «інтернет- злочини», «комп'ютерні злочини», «злочинність у сфері високих технологій», «е-злочини» тощо.

Слід зазначити, що відсутність нормативно-правового визначення ключових термінів спричиняє численні наукові дискусії. Зокрема, окремі автори вважають, що комп'ютерні злочини та кіберзлочини є різними видами злочинів у сфері високих інформаційних технологій, класифікація яких відбувається за такими ознаками: ознакою віднесення певних злочинів до комп'ютерних є знаряддя вчинення злочину – комп'ютерна техніка, зазначаючи, що об'єктом посягання є суспільні відносини у сфері автоматизованої обробки інформації; – ознакою віднесення злочинів до кіберзлочинів є специфічне середовище вчинення злочинів – кіберпростір (середовище комп'ютерних систем та мереж). Водночас об'єктом злочинного посягання можуть бути відносини будь-якої галузі людської діяльності, що має свій прояв у кіберпросторі. При цьому вказується на перелік протиправних діянь, які передбачені в Конвенції та Додатковому протоколі до неї. Відповідно, тільки діяння із цього переліку можуть бути віднесені до кіберзлочинів [5, с. 119].

Деякі вчені не погоджуються з позицією науковців, які розглядають кіберзлочини як злочини, вчинені в інформаційному середовищі, проти інформаційних ресурсів, тобто у сфері комп'ютерної інформації, або за допомогою інформаційних засобів. На думку останніх, терміни «інформаційне середовище», «інформаційні ресурси», «інформаційні засоби» є занадто загальними для сфери використання комп'ютерних систем і не розкривають суті процесів автоматизованої обробки інформації. Крім того, вчені вбачають загальною ознакою протиправних діянь, передбачених Конвенцією та Додатковим протоколом до неї, те, що їх вчинення на різних стадіях безпосередньо пов'язане з використанням ресурсів комп'ютерних систем (вчинення за допомогою комп'ютерних систем або через комп'ютерні системи), які, у свою чергу, є середовищем вчинення кіберзлочинів. Комп'ютерні дані при цьому, на їх думку, слід розглядати як інформаційний ресурс комп'ютерних систем, а комп'ютерні мережі – як різновид комп'ютерних систем. Ґрунтуючись на цій позиції, кіберзлочини слід вважати такими, що вчиняються за допомогою або через комп'ютерні системи чи пов'язані саме з комп'ютерними системами, тобто із сукупністю пристроїв, із яких один чи більше відповідно до певної програми виконують автоматичну обробку даних [6, с. 90–92].

Доцільно вказати, що поняття «кіберзлочин» вживають як синонім поняття «комп'ютерний злочин» і «злочин в сфері комп'ютерної інформації», оскільки всіх їх об'єднує одне – це використання засобів комп'ютерної техніки для вчинення злочину, проте є істотні відмінності. У той же час, в науковій літературі висвітлюється думка, що термін «кіберзлочин» набагато вужчий за поняття «злочин в сфері комп'ютерної інформації» [7, с. 85–86]. Такий підхід базується на тому, що до протиправного використання кібернетичних комп'ютерних мереж віднесено несанкціоноване отримання прав керування такою системою (наприклад, використання шкідливого програмного забезпечення, спотворення інформації про стан об'єкта в каналі зворотного зв'язку, спотворення керуючого сигналу в каналі прямого зв'язку тощо), її нерегламентоване використання (наприклад, із метою спричинення аварії на виробництві, дезорганізації діяльності підприємства тощо), а також створення та використання в злочинних цілях однієї кібернетичної комп'ютерної системи проти інших (наприклад, створення мережі зомбованих комп'ютерів для здійснення атак на вебсайти, створення несанкціонованого робочого місця в системі електронного переказу коштів тощо).

Інші вчені вказують, що кіберзлочин – найбільш небезпечне кіберправопорушення, за яке законодавством встановлюється кримінальна відповідальність [8, с. 85–86]. Таким чином вони чітко відмежували кіберзлочин та злочин, що вчиняється з використанням комп'ютерної техніки, де може й не бути кіберпростору.

На нашу думку кіберзлочини – це самостійний вид комп'ютерних злочинів, що має об'єктом різнорідні

суспільні відносини, а кіберзлочини проти власності є лише частиною всього спектра злочинів, вчинюваних у кіберпросторі.

Розкриваючи наведене, необхідно проаналізувати такі ознаки кіберзлочинів, як анонімність, транскордонність, дистанційність, а також використання комп'ютера, вірусів (інших шкідливих програм), інформаційно-телекомунікаційних мереж і кіберпростору.

По-перше, кіберзлочин, яким би способом він не вчинювався, є злочином, тобто винним, суспільно небезпечним діянням, забороненим КК України під загрозою покарання. У самому терміні «кіберзлочин» вже використовується поняття «злочин», що звільняє нас від повторення його основних ознак.

По-друге, кіберзлочин здатен завдати шкоди всім охоронюваним кримінальним законом суспільним відносинам, а не тільки відносинам у сфері комп'ютерної інформації. Отже, не варто класифікувати кіберзлочини по одному лише об'єкту посягання і просто виділити їх в окремий розділ або главу КК України.

По-третє, незважаючи на те, що кіберпростір має транскордонний характер, не всі кіберзлочини також носять транскордонний характер (наприклад, якщо винний і потерпілий живуть в одній країні). Те ж можна сказати і про такі ознаки кіберзлочинів, як анонімність або про використання шкідливих програм. Не всі кіберзлочини здійснюються анонімно, багато вчиняються відкрито з використанням реальних імен і прізвищ. Так само, як і не всі кіберзлочини вчиняються з використанням вірусів або інших шкідливих програм (вимагання в соціальній мережі або через електронну пошту). Дані ознаки кіберзлочинів є факультативними, тобто вони можуть бути притаманні лише окремим кіберзлочинам, але не всім.

Звісно ж, що об'єднуючими ознаками всіх кіберзлочинів є сфера їх вчинення – кіберпростір, інформаційно-телекомунікаційні мережі та засоби комп'ютерної техніки. Кіберпростір, як певна сфера діяльності (віртуальна реальність), може існувати лише в рамках інформаційно-телекомунікаційної мережі. Подібна мережа сформована з безлічі пристроїв і каналів зв'язку, які дозволяють отримати доступ в кіберпростір. Пристрої можуть бути різними (настільний комп'ютер, ноутбук, планшет або смартфон), як і інформаційно-телекомунікаційні мережі («Internet», «FidoNet», «CREN», «EARNet», «EUNe»). При цьому один комп'ютер може бути підключений відразу до декількох інформаційно-телекомунікаційних мереж. Тому обмежувати поняття «кіберзлочин» лише можливістю використанням персонального комп'ютера або мережі «Інтернет» є недоцільним. Злочинець може використовувати різноманітні пристрої та інформаційно-телекомунікаційні мережі для доступу саме в кіберпростір. Отже, кіберпростір є обов'язковою умовою вчинення кіберзлочинів.

Наявність інформаційно-телекомунікаційної мережі теж є обов'язковою умовою вчинення кіберзлочинів, оскільки без неї не буде кіберпростору. Використання засобів комп'ютерної техніки для доступу в кіберпростір також є невід'ємною ознакою всіх кіберзлочинів, оскільки ніяким іншим чином в кіберпростір потрапити не можна. Злочинець використовує комп'ютер в першу чергу для доступу в кіберпростір. У разі якщо винна особа просто візьме комп'ютер в руки і навмисно заподіє ним будь-кому шкоду здоров'ю, то таке діяння очевидно не можна буде назвати кіберзлочином. Отримавши доступ у кіберпростір, злочинець отримує нові можливості – тепер він здатний вчиняти злочини дистанційно, не виходячи з дому.

Звісно ж, дистанційне вчинення злочину також є невід'ємною характеристикою способу вчинення всіх кіберзлочинів. Винна особа свідомо використовує можливості кіберпростору таким чином, щоб між ним і потерпілим була безпечна відстань.

Таким чином ґрунтуючись на вищенаведеному, нами пропонується наступне визначення кіберзлочинів: під кіберзлочином доцільно розуміти злочин, що завдає шкоди різнорідним суспільним відносинам, який вчиняється дистанційно, шляхом використання засобів комп'ютерної техніки та інформаційно-телекомунікаційних мереж та за допомогою утвореного ними кіберпростору.

Пропоноване визначення розкриває поняття «кіберзлочин» через його обов'язкові ознаки, такі як засіб (кіберпростір) і спосіб (дистанційний спосіб). Також воно є ємким, оскільки не дублює всі ознаки злочину. Дане визначення не обмежено ані об'єктом посягання, ані конкретною інформаційно-телекомунікаційною мережею, що робить його досить гнучким: кіберзлочином буде вважатися як шахрайство в мережі «Інтернет», так і неправомірний доступ до комп'ютерної інформації в мережі «FidoNet» або «TOP». Дотримуючись такої логіки, кіберзлочином проти власності буде вважатися такий кіберзлочин, родовим об'єктом якого є відносини власності.

На сучасному етапі одним із найпоширеніших злочинів проти власності є шахрайство, який має динаміку до зростання як за кількісними, так і за якісними показниками. Так, якщо у 2014 р. частка цього виду злочинів проти власності від усіх посягань на власність становила 3,4%, то у 2015 р. вона була вже 17,4%. Таке зростання обсягу цього виду злочинних посягань на власність пов'язано, насамперед, зі стрімким розвитком телекомунікацій і глобальних комп'ютерних мереж, які полегшують умови вчинення злочинів проти власності та утворюють нові склади шахрайства, такі як кібершахрайство.

Як було зазначено на конгресі Організації Об'єднаних Націй з профілактики злочинності, за останні десятиліття окрема злочинна діяльність уже набула транснаціонального характеру. Деякі кримінологи пояснюють виникнення транснаціональної злочинності розширенням географічних меж, у тому числі щодо вчинення злочинів проти власності, та збільшенням кількості вчинення злочинцями кіберзлочинів (наприклад, кібершахрайств), що виходять за регіональні та національні межі [9]. Зокрема, науковці зазначають, що процеси, які відбуваються у світовій економіці XXI ст., у торгівлі, суспільно-політичному житті, є передумовою виникнення принципово нової ситуації у кримінальному світі, що знаходить своє відображення, зокрема, у появі нового виду злочинності, який належить до новітніх феноменів, що формують сучасну злочинну картину світу.

Транснаціональна злочинність може виявлятися в різних видах міжнародної злочинності. ООН опублікувала класифікацію, яка містить 17 видів міжнародних злочинних діянь, які, на думку експертів, сьогодні

справляють найбільш негативний вплив на суспільство різних держав. Зокрема, серед перших виділено й кіберзлочини проти власності.

Відповідно розвиток інформаційного простору зумовлює необхідність активізації зусиль суспільства щодо його захисту від злочинних посягань, сукупність яких уже має свою власну, відому в усьому світі назву – кіберзлочинність, що набула поширення й у сучасних умовах та становить одну з найбільш небезпечних загроз для українського суспільства. Стрімкий розвиток телекомунікацій і глобальних комп'ютерних мереж створив умови, які полегшують вчинення кіберзлочинів проти власності та утворюють нові склади. Злочинці все частіше використовують нові способи зараження комп'ютерів шкідливими програмами, які надають змогу отримувати злочинний прибуток [10, с. 208]. Так, відповідно до Звіту NCR (*Norton Cybercrime Report*), жертвами кіберзлочинності у 2012 р. стали 341 млн, а у 2015 р. – вже 594 млн осіб. Близько 70% інтернет-користувачів хоча б раз стикалися з шахрайством у Мережі, і ці показники щороку збільшуються.

Сьогодні за допомогою шкідливих комп'ютерних програм і програмно-технічних засобів, підключених до комп'ютерної мережі, можуть вчинятися більшість злочинів проти власності, передбачених розділом VI Особливої частини КК України. Виняток становлять лише злочини, спосіб вчинення яких пов'язаний з безпосереднім контактом злочинця з потерпілим, а також значна частина злочинів, предметом яких може бути лише матеріалізоване майно. Від того, що злочини проти власності вчиняються шляхом використання електронно-обчислювальної техніки та новітніх інформаційно-комунікативних технологій, вони не змінюють об'єкта свого посягання; у цьому разі відбувається приєднання додаткового об'єкта, що збільшує та якісно змінює суспільну небезпеку від злочину. У зв'язку із цим сучасна система норм, яка відображає злочини проти власності, потребує вдосконалення, оскільки вона не повною мірою враховує сучасні кіберзагрози.

Кіберзлочини проти власності мають таку ознаку, як вчинення злочину щодо великого і, як правило, невизначеного кола потерпілих. Це призводить до того, що практично неможливо точно встановити розмір завданої шкоди, а подекуди цей розмір (щодо одного потерпілого) замалий для притягнення винного до кримінальної відповідальності. Таким чином, постає запитання: чи може в такому випадку розмір шкоди бути ознакою складу злочину, яка відображає характер і міру суспільної небезпечності? Звісно, що ні. Кіберзлочини проти власності не можна кваліфікувати як замах на злочин у великому або особливо великому розмірі, оскільки згідно з кримінально-правовою теорією в цьому випадку є невизначений (неконкретизований) умисел. За таких обставин злочин потрібно кваліфікувати за наслідками, що фактично настали.

На відміну від злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, основною властивістю кіберзлочинів проти власності є те, що суб'єкт злочину використовує комп'ютерні мережі як знаряддя або засіб вчинення злочину. Саме це додає таким злочинам унікальних властивостей, не притаманних іншим злочинним посяганням. Таким чином, поняття кіберзлочинів проти власності можна визначити у вигляді сукупності заборонених кримінальним законодавством діянь, спосіб вчинення яких передбачає обов'язкове використання таких технологій (мереж) як знаряддя або засобу.

Висновки. Усе зазначене вище свідчить, що розв'язання проблеми потребує вдосконалення нормативно-правової бази, яка є підґрунтям єдиної державної політики забезпечення інформаційної (кібернетичної) безпеки та її реалізації. У зв'язку з цим, пропонуємо закріпити у чинному законодавстві поняття «кіберзлочину», під яким розуміти злочин, що завдає шкоди різнорідним суспільним відносинам, який вчиняється дистанційно, шляхом використання засобів комп'ютерної техніки та інформаційно-телекомунікаційних мереж і утвореного ними кіберпростору.

Поняття кіберзлочинів проти власності доцільно визначити як сукупність заборонених кримінальним законодавством діянь проти власності, спосіб вчинення яких передбачає обов'язкове використання кіберпростору як знаряддя або засобу.

ЛІТЕРАТУРА:

1. 165 населених пунктів підключено до безлімітного Інтернету від Укртелекому в першому півріччі 2015 року [Електронний ресурс]. – Режим доступу: http://www.ukrtelecom.ua/presscenter/news/pressrelease?id=134727.

2. Матеріали робочої зустрічі в Національній академії прокуратури України 15 вересня 2015 року.

3. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 року № 2824-IV // Відомості Верховної Ради України. – 2006. – № 5. – С. 128. – Ст. 71.

4. Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Закон України від 21 липня 2006 року № 23-V // Відомості Верховної Ради України. – 2006. – № 39. – С. 1384. – Ст. 328.

5. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): моногр. / В. Бутузов. – К.: КИТ, 2010. – 148 с.

6. Погорецький М. Кіберзлочини: до визначення поняття / М. Погорецький, В. Шеломенцев // Вісник прокуратури. – 2012. – № 8. – С. 89–96.

7. Словник термінів з кібербезпеки / за заг. ред. О. Копатіна, Є. Скулишина. – К.: Аванпост- Прим, 2012. – 214 с.

8. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: наук.-практ. посіб. / [В.М. Болгов, Н.М. Гадіон, О.З. Гладун та ін.]. – К.: Національна академія прокуратури України, 2015. – 202 с.

9. Глушков В. О. Протидія транснаціональному наркобізнесу – невід'ємна складова забезпечення безпеки людини [Електронний ресурс] / В. О. Глушков, І. М. Гриненко, Є. Д. Скулиш. – Режим доступу: http://www.nbuv.gov.ua/old_jrn/Soc_Gum/Vlduvs/2009_4/09_4_5_1.pdf.

10. Логінова Н. І. Правовий захист інформації : навч. посіб. / Н. І. Логінова, Р. Р. Дробожур. – Одесса : Фенікс, 2015. – 262 с.