УДК 343.3

Піцик Ю. М.,
секретар
Кваліфікаційно-дисциплінарної комісії прокурорів

КЛАСИФІКАЦІЯ КІБЕРЗЛОЧИНІВ ПРОТИ ВЛАСНОСТІ

Анотація. У статті розглянуто заходи, вжиті в законодавчій, інституційній сфері в Україні, напрями науково-криміналістичного забезпечення, спрямовані на боротьбу з кіберзлочинністю. Визначено поняття «кіберзлочину» проти власності та надано авторську класифікацію цієї групи злочинів.

Ключові слова: кіберзлочин, кібербезпека, класифікація кіберзлочинів, кіберзлочини проти власності.

Постановка проблеми. На сучасному етапі розвитку законодавства національного рівня відсутнє універсальне визначення «кіберзлочину». Термін «кіберзлочин» порівняно новий й утворений сполученням двох слів: «кібер» і «злочин». Термін «кібер» має на увазі поняття кіберпростору та інформаційного простору, які утворюються за допомогою комп'ютерних засобів. Кіберзлочин – це самостійний вид комп'ютерних злочинів, об'єктом якого є різнорідні суспільні відносини, а кіберзлочини проти власності є лише частиною всього спектру злочинів, які вчиняють у кіберпросторі.

Аналіз останніх досліджень і публікацій. Вивченню питання кіберзлочинності в різних аспектах присвячені наукові праці К. Бєлякова, В. Білоус, В. Бутузова, А. Войціховського, О. Волеводза, Д. Гавловського, В. Голубєва, В. Гуславського, Ю. Дорохіної, М. Литвинова, Е. Рижкова, В. Розовського, Т. Тропіної, В. Цимбалюк, О. Юхно.

Мета статті - висвітлити позиції науковців та сформувати авторську класифікацію кіберзлочинів проти власності.

Виклад основного матеріалу дослідження. Поняття «кіберзлочинність» часто вживається поряд із поняттями «комп'ютерна злочинність», «злочинність у сфері високих (інформаційних) технологій», «високотехнологічна злочинність» тощо. Кримінальний кодекс (далі – КК) України оперує терміном «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Чинне українське законодавство не містить поняття «кіберзлочину» та «кіберзлочину проти власності». Зокрема, чинним КК України передбачено кримінальну відповідальність за такі пправопорушення:

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 їхнє 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 обробляється 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 обробляється (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).

Щодо кіберзлочинів проти власності, чинний КК України передбачає відповідальність лише за злочини, передбачені ч. 3. ст. 190 КК України. Тому вітчизняне законодавство лише частково задовольняє потреби сьогодення, оскільки не містить визначення понять, які є базовими у сфері формування державної інфраструктури інформаційної безпеки, та вичерпного переліку злочинів у цій сфері.

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: зарахування певних злочинів до комп'ютерних є знаряддям вчинення злочину – комп'ютерна техніка, зазначаючи, що об'єктом посягання є суспільні відносини у сфері автоматизованої обробки інформації; 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 до цього, можемо зазначити, що лише діяння із цього переліку можуть трактуватися як кіберзлочини [1, с. 119].

Деякі вчені не погоджуються з позицією науковців, які розглядають кіберзлочини як такі, що 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 надто загальними для сфери використання комп'ютерних систем і не розкривають суті процесів автоматизованої обробки інформації. Крім того, учені вбачають загальною ознакою протиправних діянь, передбачених Конвенцією та Додатковим протоколом до неї, те, що їхнє вчинення 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 розповсюдження кіберзлочинів. Комп'ютерні дані при цьому, на їхню думку, слід розглядати

як інформаційний ресурс комп'ютерних систем, а комп'ютерні мережі – як різновид комп'ютерних систем. На основі цієї позиції, кіберзлочини варто вважати такими, що вчиняються за допомогою або через комп'ютерні системи чи пов'язані з комп'ютерними системами, тобто із сукупністю пристроїв, із яких один чи більше, відповідно до певної програми, виконує автоматичну обробку даних [2, с. 90–92].

Доцільно вказати, що поняття «кіберзлочин» вживають як синонім поняття «комп'ютерний злочин» і «злочин у сфері комп'ютерної інформації», оскільки їх об'єднує використання засобів комп'ютерної техніки для вчинення злочину. Проте є й істотні відмінності. Адже водночас із попередньою, у науковій літературі висвітлюється думка про те, що термін «кіберзлочин» вужчий за поняття «злочин в сфері комп'ютерної інформації» [3, с. 85–86]. Такий підхід базується на тому, що до протиправного використання кібернетичних комп'ютерних мереж належить 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 зі злочинною метою однієї кібернетичної комп'ютерної системи проти інших (наприклад, створення мережі «зомбованих» комп'ютерів для здійснення атак на веб-сайти, створення несанкціонованого робочого місця в системі електронного переказу коштів тощо).

Інші вчені вказують, що кіберзлочин – найбільш небезпечне кіберправопорушення, за яке законодавством встановлюється кримінальна відповідальність [4, 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 спектру злочинів, вчинюваних у кіберпросторі.

23 листопада 2001 року Рада Європи прийняла Конвенцію про кіберзлочинність [5], яку Україна ратифікувала 07 вересня 2005 року.

Вона поділяє злочини в кіберпросторі на чотири групи.

До першої групи (злочини, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних даних і систем) належать такі: незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), дія на комп'ютерні дані (ст. 4) або на системи (ст. 5), протизаконне використання спеціальних технічних пристроїв (ст. 6).

До другої належать злочини, пов'язані з використанням комп'ютерних засобів, а саме: фальсифікація та шахрайство з використанням Інтернет-технологій (ст. 7, ст. 8 Конвенцій).

Третю групу складають злочини, пов'язані з контентом (змістом) даних.

До четвертої увійшли порушення авторського та суміжних прав.

Крім того, на початку 2002 року до Конвенції додано протокол про додання до переліку злочинів поширення інформації расистського й іншого змісту, що зумовлює насильницькі дії, ненависть або дискримінацію окремої особи чи групи осіб, що грунтуються на расовій, національній, релігійній, етнічній приналежності. Таким чином, перший розділ Конвенції присвячено видам діянь, які підлягають криміналізації. Другий розділ висвітлює процесуальні аспекти боротьби з кіберзлочинністю.

Відповідно до Конвенції Ради Європи про кіберзлочинність, кіберзлочини можна умовно поділити на чотири групи:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення комп'ютерних даних, втручання в дані, втручання в систему, зловживання пристроями);

2) правопорушення, пов'язані з комп'ютерами (підробка та шахрайство, пов'язані з комп'ютерами);

3) правопорушення, пов'язані зі змістом (правопорушення, що стосуються дитячої порнографії);

4) правопорушення, пов'язані з авторськими і суміжними правами [6, ст. 2–10].

Деякі науковці пропонують поділити кіберзлочини на агресивні та неагресивні. Так, до першої групи належать кібертероризм, погроза фізичної розправи (наприклад, передана через електронну пошту), кіберпереслідування, кіберсталкінг (протиправне сексуальне домагання та переслідування іншої особи через Інтернет), дитяча порнографія (створення порнографічних матеріалів із зображенням дітей, розповсюдження цих матеріалів, отримання доступу до них). Друга група охоплює кіберкрадіжку, кібервандалізм, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусних програм [7, с. 333].

Оптимальною, на нашу думку, є класифікація кіберзлочинів, запропонована В. Дзюндзюком і Б. Дзюндзюком:

1) злочини проти конституційних прав і свобод людини та громадянина, такі як порушення недоторканості приватного житла, порушення таємниці листування, телефонних переговорів, поштових, телеграфних та інших повідомлень, авторських і суміжних прав;

2) злочини проти життя та здоров'я. Загрозливих масштабів у мережі Інтернет набуває наявність сайтів, які пропагують наркоманію, публікують технологію виготовлення наркотичних препаратів у домашніх чи промислових масштабах або які розповсюджують наркотичні засоби, психотропні речовини та їхні аналоги;

3) злочини проти честі та гідності особи. Анонімність і широка аудиторія користувачів Інтернету дають безмежні можливості для розповсюдження інформації будь-яких видів, зокрема наклепів, що порочать честь і гідність особи;

4) злочини проти власності. Одним із найпоширеніших видів злочинів на сьогодні є інтернет-шахрайство, нові форми, види і способи якого з'являються кожного дня;

5) злочини у сфері комп'ютерної інформації, такі як неправомірний доступ до інформації, створення, використання та розповсюдження шкідливих програм;

6) злочини проти суспільної моральності;

7) злочини проти безпеки держави. Із зростанням використання мережі Інтернет у державних структурах стало можливим нелегально дістати доступ не лише до приватної та корпоративної інформації, а й до інформації, що є державною таємницею, а також скоювати такі злочини, як шпигунство, державна зрада або розголошення державної таємниці [8, с. 9–10].

У спеціальній літературі висвітлюється думка, що найпоширенішими видами кіберзлочинів у сучасному світі є:

- кардинг – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів,

платіжних і розрахункових систем, а також із персональних комп'ютерів (безпосередньо або через програми віддаленого доступу, «трояни», «боти»);

- фішинг – клієнтам платіжних систем надсилаються повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи із проханням вказати свої рахунки та паролі;
- вішинг – у повідомленнях міститься прохання зателефонувати на певний міський номер, а під час розмови запитуються конфіденційні дані власника картки;
- онлайн-шахрайство – несправжні Інтернет-аукціони, Інтернет-магазини, сайти та телекомунікаційні засоби зв'язку;
- піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті;
- кард-шарінг – надання незаконного доступу до перегляду супутникового та кабельного телебачення;
- соціальна інженерія – технологія управління людьми в Інтернет–просторі;
- мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення;
- протиправний контент – контент, що пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості та насильства;
- рефайлінг – незаконна підміна телефонного трафіку [9].

Безумовно, за допомогою використання 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 із безпосереднім контактом злочинця з потерпілим, а також значна частина злочинів, предметом яких може бути лише матеріалізоване майно.

Через те, що злочини проти власності вчиняються шляхом використання електронно-обчислювальної техніки та новітніх інформаційно-комунікативних технологій, вони не змінюють об'єкт свого посягання. У цьому разі відбувається приєднання додаткового об'єкту, що збільшує та якісно змінює суспільну небезпеку від злочину. У зв'язку з цим сучасна система норм, яка відображає злочини проти власності, потребує вдосконалення, оскільки вона не повною мірою враховує сучасні кіберзагрози.

Кіберзлочини проти власності характеризуються такою ознакою, 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. На відміну від злочинів у сфері використання електронно-обчислювальних машин, 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 [10, с. 40–42].

Залежно від способу вчинення кіберзлочини проти власності можна розділити на такі групи:

1) кіберзлочини проти власності, що вчиняють шляхом психологічного впливу на людину (обман, введення в оману, загроза);

2) кіберзлочини проти власності, що вчиняють шляхом «впливу» на обладнання (комп'ютери, смартфони та інше обладнання).

Такий поділ обумовлюється тим, що до першої групи належать такі суспільно небезпечні діяння, під час вчинення яких заподіюється шкода тільки одному безпосередньому об'єкту – відносинам власності. Під час вчинення кіберзлочинів проти власності другої групи злочинець завдає шкоди ще й додатковому об'єкту – відносинам, які складаються у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку.

Кіберзлочини першої групи відрізняються тим, що під час їхнього вчинення використовують вже наявні сайти, форуми й готові програми. Злочинці «працюють» з тим, що їм надає власне кіберпростір. До таких кіберзлочинів можна зарахувати шахрайство, вимагання, заподіяння майнової шкоди шляхом обману та зловживання довірою.

Спосіб вчинення цих кіберзлочинів проти власності мало чим відрізняється від способу вчинення аналогічних злочинів в матеріальному світі: за умов шахрайства – обман або зловживання довірою; під час вимагання – загроза і т. ін. Обман у кіберпросторі має таку ж суспільну небезпеку, що й обман в матеріальному світі, лише перший вчиняється дистанційно. Так само і з погрозами, і з іншими способами вчинення таких злочинів проти власності.

До злочинів другої групи можна зарахувати злочини, під час вчинення яких особа може використовувати спеціальні програми, що дозволяють безперешкодно отримати неправомірний доступ до комп'ютерної інформації («BruteForce», «Public Brute / Checker») або використовувати віруси («Creeper», «Elk Cloner», «Brain», «Jerusalem», «March6», «CIH», «Nimda»), троянські програми («Win64 / HackKMS.A»), комп'ютерні хробаки («Melissa», «Sasser», «My Doom», «Conficker») та інші шкідливі програми.

Використовуючи шкідливе програмне забезпечення при вчинені кіберзлочинів проти власності, винна особа посягає одразу на два об'єкти – відносини власності й відносин у сфері використання електронно–обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку. Звісно ж ця обставина підвищує їхню суспільну небезпеку. Саме це додає таким злочинам унікальних властивостей, непритаманних для інших злочинних посягань.

Таким чином, поняття кіберзлочинів проти власності можна визначити як сукупність заборонених кримінальним законодавством діянь, спосіб вчинення яких передбачає обов'язкове використання таких технологій (мереж) як знарядь або способів. На основі проведеного аналізу, пропонуємо таку класифікацію кіберзлочинів проти власності залежно від способу вчинення:

– кіберзлочини проти власності, що вчиняються шляхом психологічного впливу на людину з використанням комп'ютерної та іншої аналогічної техніки (обман, введення в оману, загрози);

– кіберзлочини проти власності, що вчиняються шляхом впливу на обладнання (комп'ютери, смартфони, маршрутизатори та інше обладнання).

Висновки. Підсумовуючи вищенаведене, слід підкреслити, що кіберзлочинність є вкрай небезпечним соціальним явищем, яке становить загрозу світового масштабу. На сьогодні боротьба з кіберзлочинністю проти власності є одним із пріоритетних напрямків діяльності правоохоронних органів держави, але для комплексної протидії її необхідно, перш за все, узгодити на національному рівні та законодавчо закріпити термінологію,

яка безпосередньо стосується кіберзлочинності, зокрема визначення ключових понять «кіберзлочин» і, відповідно, «кіберзлочин проти власності».

Література:

1. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно–структурний аналіз): монографія. Київ: КИТ, 2010. 148 с.
2. Погорецький М. Кіберзлочини: до визначення поняття. Вісник прокуратури. 2012. № 8. С. 89–96.
3. Словник термінів з кібербезпеки / за заг. ред. О. Копатіна, Є. Скулишина. Київ: Аванпост–Прим, 2012. 214 с.
4. Болгов В., Гадіон Н., Гладун О. Організаційно–правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: наук.–практ. посіб. Київ: Національна академія прокуратури України, 2015. 202 с.
5. Конвенція про кіберзлочинність від 23 листопада 2011 року. URL: http://zakon5.rada.gov.ua/laws/show/994_575/print1453722395322329.
6. Конвенція про кіберзлочинність: від 23.11.2001. БД «Законодавство України» / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/994_575.
7. Голіна В., Головкін Б. Кримінологія: Загальна та Особлива частини: навч. посіб. Харків: Право, 2014. 513 с.
8. Дзюндзюк В., Дзюндзюк Б. Поява і розвиток кіберзлочинності. URL: http://nbuv.gov.ua/j–pdf/DeBu_2013_1_3.pdf.
9. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. URL:: http://www.gurt.org.ua/articles/34602.
10. Дорохіна Ю. До проблеми розуміння кіберзлочинів проти власності. Кібербезпека в Україні: правові та організаційні питання: матеріали всеукр. наук.–практ. конф. (Одеса, 21 жовтня 2016 р.). Одеса: ОДУВС, 2016. 233 с.

Пицык Ю. Н. Классификация киберпреступлений против собственности

Аннотация. В статье рассмотрены меры, принятые в законодательной и институционной сфере в Украине, направления научно-криминалистического обеспечения, обращенные на борьбу с киберпреступностью. Определено понятие киберпреступлений против собственности и предоставлена авторская классификация этой группы преступлений.

Ключевые слова: киберпреступность, кибербезопасность, классификация киберпрестпулений, киберпреступления против собственности.

Pitsyk Yu. Classification of cybercrimes against property

Summary. This article is about the measures which were taken in the domestic legislative, institutional spheres in Ukraine and scientific-criminalistic guarantee with the aim to struggle the cybercrime. The concept of cybercrime against property is defined and the author's classification of this group of crimes is provided.

Key words: cybercrime, cybersecurity, cybercrimes classification, cybercrime against property.