УДК 343.2/.7

Ричка Д. О.,
аспірант ІІІ курсу юридичного факультету
Дніпровського національного університету імені Олеся Гончара

ПРОЯВИ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН, СИСТЕМ, КОМП'ЮТЕРНИХ МЕРЕЖ ТА МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

MANIFESTATIONS OF ORGANIZED CRIME IN THE FIELD OF USE OF ELECTRONIC COMPUTING MACHINES, SYSTEMS, COMPUTER NETWORKS AND ELECTRICITY NETWORK

У науковому дослідженні розглядаються особливості, притаманні організованій злочинності у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку. Досліджено стан організованих груп та злочинних організацій, притаманні їм ознаки, розподіл ролей між співучасниками, на підставі чого сформовано пропозиції щодо вдосконалення норм чинного законодавства.

Ключові слова: *організована комп'ютерна злочинність, хакери, віртуальні банди, кібербанди, кіберугрупування, комп'ютерні підпілля.*

В научном исследовании рассматриваются особенности, присущие организованной преступности в сфере использования электронно-вычислительных машин, систем, компьютерных сетей и сетей электросвязи. Исследовано состояние организованных групп и преступных организаций, их признаки, распределение ролей между соучастниками, на основании чего сформированы предложения по усовершенствованию норм действующего законодательства.

Ключовые слова: организованная компьютерная преступность, хакеры, виртуальные банды, кибербанды, кибергруппировки, компьютерное подполье.

The scientific research deals with the peculiarities of organized crime in the sphere of the use of electronic computers, systems, computer networks and telecommunication networks. The state of organized groups and criminal organizations, the features inherent to them, distribution of roles among accomplices, on the basis of which the proposals on the improvement of the norms of the current legislation are formed.

Key words: *organized computer crime, hackers, virtual gangs, cyber gangs, cyber groupings, computer underground.*

Постановка проблеми. Проведення наукового аналізу кримінально-правової відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, які вчиняються організованими групами та злочинними організаціями, є передумовою ефективної протидії організованій комп'ютерній злочинності.

Ступінь розробленості проблеми. Окремим питанням організованої злочинності у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку присвячено праці видатних учених, а саме: Р. Дремлюги, В. Хахановського, М. Коржанського, Т. Міхайліної, В. Телійчука, О. Поливоди, А. Кузнецова, О. Долженкова, Е. Хвостика, А. Осипенко, В. Шеломенцева, Д. Злобіна.

У вищезазначених здобутках учених висвітлено переважно загальні риси організованої злочинності, на нашу думку, організована злочинність у цій сфері наділена підвищеною суспільною небезпекою. Саме тому метою дослідження є вдосконалення норм чинного кримінального законодавства у розрізі організованої злочинності у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Виклад основного матеріалу. Під організованою злочинністю слід розуміти сукупність злочинів, що вчиняються у зв'язку зі створенням та діяльністю організованих злочинних угруповань [1, ст. 1]. Під організованою комп'ютерною злочинністю мається на увазі сукупність комп'ютерних злочинів, що вчиняються у зв'язку зі створенням та діяльністю організованих злочинних угруповань. Кіберзлочинність наділена високою соціальною небезпечністю, що випливає з кола суспільних відносин, яким вона загрожує, її транснаціонального та організованого характеру [2, с. 24; 3, с. 79], складністю виявлення, встановлення наявності вини та отриманням доказів.

Відповідно до статті 28 КК України злочин визнається вчиненим організованою групою, якщо в його готуванні або вчиненні приймали участь декілька осіб (три і більше), які попередньо зорганізувалися у стійке об'єднання для вчинення певного комп'ютерного злочину та інших злочинів у подальшому, об'єднаних єдиним планом із розподілом функцій учасників групи, спрямованих на досягнення плану, відомого усім учасникам такої групи [4]. Зазначені дії включають пошук співучасників, об'єднання зусиль, детальний розподіл між ними обов'язків, складення плану, визначення способів його виконання. При цьому основною метою організатора такої групи (організації) є утворення стійкого об'єднання осіб для заняття злочинною діяльністю (вчинення комп'ютерних злочинів), забезпечення

взаємозв'язку між діями всіх учасників, упорядкування взаємодії його структурних частин [5].

До таких ознак притаманних злочинним організаціям науковець Коржанський М. Й., відносить:

1) наявність статуту – розробленого і схваленого учасниками групи плану злочинної діяльності та визначення мети діяльності групи;

2) наявність організатора (керівника);

3) конспірація (приховування) – прикриття своєї діяльності;

4) вербування нових членів;

5) наявність загальних правил поведінки, ієрархія стосунків між учасниками групи;

6) наявність матеріальної бази [6, с. 92].

Організовані співтовариства доцільно називати кіберугрупуваннями, адже вони мають свою ієрархію, статут і розподіл ролей між учасниками. Деякі вчені застосовують термін «кібербанда», проте, на нашу думку, це недоцільно, адже бандою визнається озброєна група/злочинна організація, яка попередньо створена з метою вчинення кількох нападів на підприємства, установи, організації чи на окремих осіб або для одного такого нападу, який потребує ретельної довготривалої підготовки. Зважаючи на віртуальність комп'ютерних злочинів, наявність зброї практично виключається.

Співучасниками комп'ютерних злочинів є організатор, виконавець, підбурювач та пособник [4]. Організатори злочинних груп у більшості випадках не вчиняють злочинів самотужки, а виступають у ролі координаторів проектів, під керівництвом яких розробляються плани атак, створюється шкідливе програмне забезпечення, збирається конфіденційна інформація про осіб, яка потім реалізується на «чорному ринку» [7; 8, с. 190].

Організатором є особа, яка організувала вчинення злочину (злочинів) або керувала його (їх) підготовкою чи вчиненням; утворила організовану групу/злочинну організацію або керувала нею; особа, яка забезпечувала фінансування чи організовувала приховування злочинної діяльності організованої групи або злочинної організації [4]. Саме організатор, як справедливо зазначають Л.Д. Гаухман і С.В. Максимов, створює групу, здійснює підбір співучасників, розподіляє ролі між ними, встановлює дисципліну і т.д.

Дії організатора злочину (злочинів) у простій формі співучасті належить кваліфікувати за статтею Особливої частини КК, якою передбачена відповідальність за вчинений злочин із посиланням на ч. 3 ст. 27 КК, а якщо він був одним із виконавців діянь, що становлять об'єктивну сторону складу цього злочину, – без посилання на зазначену норму. Якщо ж особа брала участь у вчиненні одного злочину як організатор, а іншого – як виконавець, пособник чи підбурювач, його дії в кожному випадку мають кваліфікуватися самостійно [5].

Особливістю організованої групи є те, що кожен співучасник виконує дії, доцільні для всієї групи. До складу організованої групи можуть входити особи, які виконують управлінські функції в організаціях, посадові особи та інші службовці. Участь таких суб'єктів у вчиненні комп'ютерних злочинів може помітно полегшити підготовку і вчинення неправомірного доступу до комп'ютерної інформації, а також приховати такий злочин.

Особливістю організованої кіберзлочинності є обов'язкова наявність специфічного учасника злочинної групи – хакера (фрікера, крекера тощо). Саме так називають особу, яка володіє знаннями й навичками несанкціонованого проникнення до комп'ютерної системи. Він і є основним виконавцем злочинного діяння [9; с. 199; 10, 32–33].

Сьогодні є чимало кіберугрупувань та хакерських злочинних рухів, однією з яких є кіберугрупування, організоване українцем, – Infroud. Зловмисники створили розгалужену й добре організовану мережу, яка протизаконним шляхом отримувала особисті дані інтернет-користувачів, які надавали доступ до банківських та електронних рахунків. За час існування угруповання злочинці завдали своїми діями збитків на понад $530 млн. Наразі слідчі вважають причетними до злочинного угруповання загалом 36 осіб. 13 членів кібербанди вже заарештували. Арешти проводилися в США, Австралії, Британії, Франції, Італії, Косові, Сербії та Албанії. Після чого співробітники правоохоронних органів США припинили діяльність злочинного угруповання [11].

Несанкціонований доступ до інформації в автоматизованих (комп'ютерних) системах є одним із найпоширеніших злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, мереж електрозв'язку. Розповсюдження сучасних електронних засобів та простота їх управлінням може призвести до потенційних загроз усунення захисту інформації в автоматизованих системах, зокрема таких, що становлять мережі телекомунікацій. До того ж виникають обставини, які зумовлюють ланцюгову реакцію щодо несанкціонованого витоку інформації, її блокування, спотворення чи знищення інформації у комп'ютерній формі [12, с. 89; 10, с. 34].

Банківська система держави пов'язана з накопиченням, розподілом і використанням державних та приватних коштів, отже є однією з найбільш привабливих для злочинців та особливо організованих злочинних груп. Злочини, що вчиняються в банківській системі або з її використанням, можна віднести до одних із найбільш небезпечних економічних злочинів, оскільки їх негативний вплив відображається не лише на банку, а й на інших суб'єктах економічної діяльності та фінансовій системі держави загалом.

Способи вчинення банківських злочинів різноманітні, найбільш розповсюджені з них такі, що вчиняються з використанням сучасних інформаційних технологій: підробка та використання пластикових платіжних карток та комп'ютерної банківської інформації. Відомою нині є діяльність міжнародної кібермережі Avalanche, яка спеціалізувалася на кібератаках із метою крадіжки пін-кодів, даних кредиток, розсилки спаму, DDoS-атак та ін. Збитки від діяльності Avalanche сягають сотень мільйонів євро.

Цікаво й те, що в міжнародну кібермережу увійшло три українці та, незважаючи на наявні докази, керівника злочинної організації, попередньо затриманого, відпустили [13].

Особливістю злочинів у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є те, що вони можуть вчинятися з використанням засобів комунікацій віддаленого доступу, не потребується присутність правопорушників на безпосередньому місці вчинення злочину. Адже особливість глобальної мережі – відсутність кордонів. Останнім часом спостерігається тенденція до зрощення комп'ютерної злочинності з традиційною організованою злочинністю, інтернаціоналізації цього виду злочинів, що підвищує рівень суспільної небезпеки. Дедалі частіше спостерігається тенденція до об'єднання хакерів у групи, які мають чітко виражені ознаки організованих злочинних угруповань [14; 15, с. 113; 3, с. 81–82]. Хакерська субкультура за своєю суттю є унікальним явищем, яке не має аналогів. Використанням комунікаційних можливостей сучасних глобальних мереж для обміну кримінальним досвідом та координації своєї діяльності якісно відрізняє організовану комп'ютерну злочинність від інших видів злочинів.

У мережі створюються спеціальні місця спілкування: форуми, конференції хакерської тематики, спеціалізовані сайти. Нерідко відвідування таких місць може бути обмежено та захищено певними паролями. Така обставина дозволяє західним дослідникам для опису такого соціального явища використовувати поняття «комп'ютерне підпілля», що означає особливе соціальне середовище особистостей, які, хоч і діють окремо, але підтримують один одного за рахунок спільного використання інформаційних ресурсів [16, с. 35]. У хакерському середовищі розповсюджено використання псевдонімів із метою приховання справжніх імен. Зв'язки у злочинних угрупованнях можуть мати як тимчасовий, так і постійний характер із чіткою ієрархією та розподілом ролей у виконанні протиправного посягання [8, с. 190; 17, с. 136].

Розподіл ролей у комп'ютерній організованій злочинності та дослідження ролі організатора попередньо було окреслено, тому перейдемо до інших ймовірних учасників організованої комп'ютерної злочинності.

Виконавцем (співвиконавцем) є особа, яка у співучасті з іншими суб'єктами злочину безпосередньо чи шляхом використання інших осіб, що відповідно до закону не підлягають кримінальній відповідальності за скоєне, вчинила злочин, передбачений КК України [4]. Наприклад, у березні 2018 року працівниками кіберполіції було встановлено причетність 30-річного мешканця Києва до розробки вірусів, кібершпигунства та продажу персональних даних громадян з усього світу. Також хакер збував шкідливе програмне забезпечення та створював віруси, які використовувалися для отримання віддаленого доступу до комп'ютерів жертв та подальшого всебічного контролю над ними. Поліцейськими було встановлено, що чоловік є учасником хакерського угруповання «Cobalt», члени якого причетні до масових атак на різноманітні світові банки. До його обов'язків входили розробка та підтримання належної роботи експлойтів, які використовували вразливості у найбільш розповсюджених серед користувачів програмних продуктах. Тобто ми спостерігаємо чіткий розподіл ролей учасників. У межах кримінального провадження розпочатого за ст. 361 КК України встановлюються особи, яким зловмисник продавав шкідливе програмне забезпечення та допомагав в отриманні повного контролю над комп'ютерною технікою жертв [18].

У такому разі описане злочинне діяння підпадає під вчинення злочину виконавцем, попередню кваліфікацію, за якою доцільно проводити за статтею 361-1 Кримінального кодексу України «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут».

Підбурювачем є особа, яка умовлянням, підкупом, погрозою, примусом або іншим чином схилила іншого співучасника до вчинення злочину [4]. Не таємниця, що організовані злочинні угруповання мають у своїх «штатах» спеціалістів, які займаються розвідкою з використанням найсучасніших технічних засобів для збирання необхідної інформації про діяльність конкурентів, засобів масової інформації, підприємств та фірм, які перебувають у межах їх інтересів, і правоохоронних органів. Серед комп'ютерних злочинів, які вчиняються у світі, все більше стає «міжнародних», таких, які як засоби або жертви використовують інформаційні системи різних держав світу з можливістю доступу до національних, зокрема спеціально захищених інформаційних ресурсів, що створює нові умови для організованої злочинності – використання мережі Інтернет не тільки для здійснення правопорушень, а й для організації віртуальних банд. Таких учасників доцільно називати пособниками.

Пособником визначається особа, яка порадами, вказівками, наданням засобів чи знарядь або усуненням перешкод сприяла вчиненню злочину іншими співучасниками, а також особа, яка заздалегідь обіцяла переховати злочинця, знаряддя чи засоби вчинення злочину, сліди злочину чи предмети, здобуті злочинним шляхом, придбати чи збути такі предмети, або іншим чином сприяти приховуванню злочину [4].

Злочин визнається вчиненим злочинною організацією, якщо його було скоєно стійким ієрархічним об'єднанням декількох осіб (п'яти і більше), члени або структурні частини якого за попередньою змовою зорганізувалися для спільної діяльності з метою безпосереднього вчинення тяжких або особливо тяжких злочинів учасниками цієї організації, або керівництва чи координації злочинної діяльності інших осіб, або забезпечення функціонування як самої злочинної організації, так й інших злочинних груп Відповідно до статті 255 КК, створення злочинної

організації з метою вчинення тяжкого чи особливо тяжкого злочину, а також керівництво такою організацією або участь у ній, участь у злочинах, вчинюваних такою організацією, а також організація, керівництво чи сприяння зустрічі (сходці) представників злочинних організацій або організованих груп для розроблення планів і умов спільного вчинення злочинів, матеріального забезпечення злочинної діяльності чи координації дій об'єднань злочинних організацій або організованих груп уже є злочином та караються позбавленням волі на строк від п'яти до дванадцяти років [4].

Стійкість організованої групи та злочинної організації полягає в їх здатності забезпечити стабільність і безпеку свого функціонування, тобто ефективно протидіяти факторам, що можуть їх дезорганізувати, як внутрішнім (наприклад, невизнання авторитету або наказів керівника, намагання окремих членів об'єднання відокремитись чи вийти з нього), так і зовнішнім (недотримання правил безпеки щодо дій правоохоронних органів, діяльність конкурентів у злочинному середовищу тощо). На здатність об'єднання протидіяти внутрішнім дезорганізувальним факторам указують такі ознаки: стабільний склад, тісні стосунки між його учасниками, їх централізоване підпорядкування, єдині для всіх правила поведінки, а також наявність плану злочинної діяльності і чіткий розподіл функцій учасників щодо його досягнення.

Ознаками зовнішньої стійкості злочинної організації можуть бути встановлення корупційних зв'язків в органах влади, наявність каналів обміну інформацією щодо діяльності конкурентів у злочинному середовищі, створення нелегальних (тіньових) страхових фондів та визначення порядку їх наповнення й використання тощо.

У складі злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку найбільшу небезпеку для суспільства, осіб та держави становлять злочини, що мають ознаки організованої злочинності: комп'ютерний тероризм; диверсія, інші прояви антагоністичної інформаційної боротьби кримінальних формувань із державою, правоохоронними органами; крадіжки інформації з баз даних та комп'ютерних програм; шахрайства з використанням комп'ютерних технологій, особливо у сфері міжнародних економічних відносин (кредитно-фінансова, банківська) тощо [19, с. 56] .

Одним із таких кіберугрупувань визнано Sofacy Group, його відносять до типу розвиненої сталої загрози. Злочинне угрупування спеціалізується на кібершпигунстві за військовими та політичними установами, викраденні інформації, що становить інтерес із точки зору оборони та геополітики. Серед відомих жертв угрупування є Національний комітет Демократичної партії США, Німецький парламент, французька компанія TV5Monde, міжнародна антидопінгова асоціація WADA. Окрім організацій, угрупування атакувало окремих приватних осіб, впливових людей у політичному середовищі східної Європи, України, офіційних осіб НАТО та хактевістів, чеченські організації та ін. [20].

Організована комп'ютерна злочинність є серйозною загрозою державного рівня. Особливість, притаманна кіберзлочинам, які вчинені у складі організованих груп чи злочинних угрупувань, полягає у підвищеній суспільній небезпеці. На тлі віртуальності комп'ютерної злочинності, злочинці мають можливість організовувати свою діяльність на досить великих відстанях.

Висновок. Має сенс доповнити статті розділу XVI КК України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» кваліфікувальними складами за вчинення комп'ютерних злочинів організованими групами та злочинними організаціями, підсилюючи кримінальну відповідальність за умови використання службового становища, не тільки щодо статті 362 КК, а й до інших норм розділу. Доцільно проводити кваліфікацію за сукупністю норм КК за статтею розділу XVI КК та статтею 255 КК України на тлі підвищеної суспільної небезпеки.

ЛІТЕРАТУРА:

1. Закон України «Про організаційно-правові основи боротьби з організованою злочинністю» від 30.06.1993 № 3341-XII (у редакції від 05.01.2017). URL: http://zakon2.rada. gov.ua/laws/show/3341-12.

2. Дремлюга Р.И. Интернет-преступность: автореф. дис. на соискание ученой степени канд. юрид. наук: спец. 12.00.08 «Уголовное право и криминология; Уголовно-исполнительное право». Владивосток, 2007. 26 с.

3. Хахановський В.Г. Проблеми боротьби з організованою кіберзлочинністю в економічній сфері/ Боротьба з організованою злочинністю і корупцією (теорія і практика). № 2 (30), 2013. С. 79–83.

4. Кримінальний Кодекс України від 05.04.2001 № 2341-III (у редакції від 07.03.2018 № 2341-14). URL: http://zakon3.rada.gov.ua/laws/show/2341-14.

5. Постанова Пленуму ВСУ України «Про практику розгляду судами кримінальних справ про злочини, вчинені стійкими злочинними об'єднаннями» від 23.12.2005р. N 13. URL: http://zakon2.rada.gov.ua/laws/show/v0013700-05.

6. Коржанський М. Й. Кваліфікація злочинів: [навч. посіб.]. Вид. 3-тє, доповн. та переробл. Київ: Атіка, 2007. 592 с.

7. Киберпреступность становится более организованной. URL: http://www.crimeresearch. ru/news/17.07.2008/4632/.

8. Міхайліна Т. Особливості кваліфікації злочинів із використанням засобів комп'ютерної техніки, що вчиняються групою осіб. Публічне право. № 3. 2011. С. 183–193.

9. Телійчук В.Г. Протидія злочинам, що вчиняються організованими злочинними угрупованнями з використанням комп'ютерних технологій// Організація і тактика документування підрозділами ДСБЕЗ злочинів у комп'ютерних мережах та мережах електрозв'язку: матеріали всеукр. наук.-практ. конф., м. Донецьк, 4 грудня 2009 р. / Донецький юрид. ін-т ЛДУВС ім. Е.О. Дідоренка. Донецьк: ДЮІ ЛДУВС, 2009. С. 198–202.

10. Телійчук В.Г. Способи вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та заходи протидії. Держава та регіони. Серія: Право, № 2 (44), 2014. С. 31–37.

11. США спіймали організовану українцем кібербанду, яка накрала $530 млн/ Сайт depo.ua. URL: https://www.depo.ua/ukr/life/ssha-spiymali-organizovanu-ukrayincem-kiberbandu-yaka-nakrala-530-mln-20180208723213.

12. Поливода О.Ю. Боротьба з комп'ютерною злочинністю в Україні: проблемні питання // Взаємодія правоохоронних органів з провайдерами та операторами зв'язку в боротьбі з комп'ютерними злочинами: матеріали регіонального наук.-практ. семінару, м. Донецьк, 12 грудня 2008 р. / Донецький юрид. ін-т ЛДУВС ім. Е.О. Дідоренка. Донецьк: ДЮІ ЛДУВС, 2009. С. 88–91.

13. Суд Полтави відпустив хакера кібербанди Avalanche, розшукуваного 4 роки у 30 країнах світу – ЗМІ/ Сайт Новое время. URL: https://nv.ua/ukr/ukraine/events/sud-poltavi-vidpustiv-hakera-kiberseti-avalanche rozshukuvanogo-4-roki-u-30-krajinah-svitu-zmi-303223.html.

14. Кузнецов А. Борьба с преступлениями, совершаемыми с использованием сети Интернет. URL: http://www.security.ukrnet.net/modules/sections/index.php?op=viewarticle&artid=593.

15. Долженков О.Ф. Інфраструктура організованої економічної злочинності. Одеса: НДРВВ ОЮІ НУВС, 2002. 254 с.

16. Осипенко А.Л. Хакерское сообщество в глобальных компьютерных сетях как криминологический феномен. Современное право. 2006. № 5. С. 35–39.

17. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт. Москва, 2004. С. 135–138.

18. Кіберполіція викрила українського хакера у взламі комп'ютерів світових банків та готелів/ Офіційний сайт Національної поліції. URL: https://www.npu.gov.ua/news/kiberzlochini/ kiberpolicziya-vikrila-ukrajinskogo-xakera-u-vzlami-komp-yuteriv-svitovix-bankiv-ta-goteliv/. 02.04.2018р.

19. Злобін Д.Л. Взаємодія операторів мобільного зв'язку з ОВС при розслідуванні комп'ютерних злочинів/ Матеріали регіонального наук.-практ. семінару, м. Донецьк, 12 грудня 2008 р. / Донецький юрид. ін-т ЛДУВС ім. Е.О. Дідоренка. Донецьк: ДЮІ ЛДУВС, 2009. С. 56–61.

20. Sofacy Group. URL: https://uk.wikipedia.org/wiki/Sofacy_Group.