УДК 343.6
DOI https://doi.org/10.24144/2788-6018.2023.06.106

ОСОБЛИВОСТІ КВАЛІФІКАЦІЇ ОРГАНІЗОВАНОЇ КОМП'ЮТЕРНОЇ ЗЛОЧИННОСТІ В УКРАЇНІ

Саморай О.К.,
аспірант кафедри права
приватного вищого навчального
закладу «Європейський університет»,
ORCID: 0009-0000-3384-155X

Саморай О.К. Особливості кваліфікації організованої комп'ютерної злочинності в Україні.

У даній статті проведено аналіз особливостей, притаманних кримінально-правовій кваліфікації кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, які мають груповий характер. Констатовано, що їх особливостями є високотехнологічність, латентність, зазвичай груповий характер та високий рівень суспільної небезпечності, що зумовлює складність виявлення та розслідування відповідних злочинів, притягнення усіх учасників угруповання до кримінальної відповідальності. Зазначається, що під організованою комп'ютерною злочинністю слід розуміти сукупність комп'ютерних злочинів, що вчиняються у зв'язку зі створенням та діяльністю організованих злочинних угруповань. Встановлено, що співучасниками комп'ютерних злочинів є організатор (здебільшого координатори проєктів, під керівництвом яких розробляються плани атак, створюється шкідливе програмне забезпечення, збирається конфіденційна інформація про осіб з метою реалізації на «чорному ринку» тощо), виконавець, підбурювач та пособник. Підкреслено, що особливим суб'єктом зазначених злочинів є хакер, який зазвичай є виконавцем злочину. Наведено аргументи, що проміжок часу між змовою і початком вчинення суспільно небезпечних дій у кожного з виконавців комп'ютерного злочину не відіграє ключову роль, водночас повинні бути встановлені умисел на попередньо обговорені узгоджені дії, які необхідні для досягнення злочинного результату. Виявлено тенденцію до збільшення кількості комп'ютерних злочинів з використанням засобів комунікації віддаленого доступу, об'єднанням хакерів у групи, які мають ознаки організованих злочинних угруповань, використанням спеціально створених місць для спілкування (форумів, спеціалізованих сайтів та інше), наявністю чіткої ієрархії та розподілу ролей у виконанні протиправних дій.

Ключові слова: комп'ютерні злочини, кваліфікація, організована злочинність, розслідування, запобігання.

Samorai O.K. Features of the qualification of organized computer crime in Ukraine.

This article analyzes the features inherent in the criminal qualification of criminal offenses in the field of use of electronic computing machines (computers), systems and computer networks and telecommunication networks that are of a group nature. It was established that their features are high technology, latency, usually a group nature and a high level of public danger, which makes it difficult to identify and investigate relevant crimes, bring all members of the group to criminal responsibility. It is noted that organized computer crime should be understood as a set of computer crimes committed in connection with the creation and activities of organized criminal groups. It has been established that accomplices in computer crimes are the organizer (mostly project coordinators, under whose leadership attack plans are developed, malicious software is created, confidential information about individuals is collected for the purpose of sale on the "black market", etc.), executor, instigator and accomplice. It is emphasized that the special subject of these crimes is a hacker, who is usually the perpetrator of the crime. Arguments are given that the time interval between the conspiracy and the beginning of the commission of socially dangerous actions for each of the perpetrators of the crime does not play a key role, at the same time, the intention of prediscussed concerted actions, which are necessary to achieve a criminal result, must be established. The tendency to increase the number of computer crimes with the use of remote access communication tools, the unification of hackers in groups that have signs of organized criminal groups, the use of specially created places for communication (forums, specialized sites, etc.), the presence of a clear hierarchy and distribution was revealed roles in the execution of illegal actions.

Key words: computer crimes, qualification, organized crime, investigation, prevention.

Постановка проблеми. Однією з провідних тенденцій розвитку людської цивілізації протягом останніх десятиліть стало прискорення тех-

нологічного прогресу, насамперед інформаційно-телекомунікаційних технологій, що сприяли віднайденню нових рішень правових, економічних та соціальних проблем сучасності. Водночас, поява нових можливостей зазвичай супроводжується новими ризиками та загрозами для суспільних відносин. Зі збільшенням активності у використанні комп'ютерних мереж збільшується вірогідність їх використання з метою вчинення кримінальних правопорушень [1, с. 2] – нового різновиду суспільно-небезпечних діянь, які в кримінальному праві були об'єднані у групу злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку [2, с. 2].

Протягом останніх років в Україні спостерігається стійка тенденція щодо зростання кількості злочинів, учинених у сфері використання комп'ютерів, комп'ютерних мереж та мереж електрозв'язку, щодо яких уживається узагальнена назва «комп'ютерні злочини» [3], простежується організований та транснаціональний характер, удосконалюються способи їх вчинення. Зазначені обставини, а також низький відсоток розкриття зазначених злочинів актуалізує доцільність з'ясування особливостей кваліфікації організованої комп'ютерної злочинності в Україні з метою вироблення ефективних методів протидії.

Стан опрацювання. Питання кваліфікації злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку стали предметом досліджень таких вітчизняних науковців, як Д.С. Азаров, П.Д. Біленчук, Л.В. Борисова, М.В. Карчевський, М.Й. Коржанський, С.А. Кузьмін, Т.М. Луцький, С.С. Мірошниченко, О.Ф. Пасєка, О.Е. Радутний, Д.О. Ричка, Т.І. Созанський, С.В. Шапочка та ін.

Віддаючи належне науковому доробку зазначених науковців, на сьогодні залишаються невирішеними чимало проблем у здійсненні кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, учинених групою осіб. Це вказує на актуальність і своєчасність досліджуваної проблеми, необхідність вивчення кримінально-правової кваліфікації зазначених злочинних посягань, які мають груповий характер, з метою побудови моделі запобігання.

Мета статті полягає у визначенні особливостей, притаманних кримінально-правовій кваліфікації кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, які мають груповий характер, і розробці пропозицій щодо запобігання їм.

Виклад основного матеріалу. Кримінальні правопорушення, що посягають на суспільні відносини щодо забезпечення контрольованого використання комп'ютерної інформації та нормальної роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку законодавець виокремив у розділ XVI Кримінального кодексу України [4].

Однією з найбільш розповсюджених кваліфікуючих ознак (ч. 2 ст. 361, ч. 2 ст. 361-1 КК, ч. 2 ст. 361-2 КК, ч. 2 ст. 362 КК України) злочинів є вчинення їх за попередньою змовою групою осіб. 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, скоєних у складі організованих груп та злочинних організацій є передумовою ефективної боротьби з організованою комп'ютерною злочинністю.

Відповідно до положень ст. 28 КК України злочин вважається таким, що вчинений групою осіб, якщо у ньому брали участь декілька (два або більше) виконавців без попередньої змови між собою. Злочин визначається вчиненим за попередньою змовою групою осіб, якщо його вчинили декілька осіб (два або більше), які заздалегідь, тобто до початку злочину, домовилися про спільне його вчинення [4].

До характерних ознак, притаманних злочинним групам, слід віднести: взаємну погодженість дій всіх учасників групи; наявність змови про спільне вчинення злочину; взаємна усвідомленість вчинення злочину спільними зусиллями; наявність суб'єктивного зв'язку між членами групи; участь у вчиненні злочину декількох суб'єктів.

Як слушно вказує Л.В. Борисова, розширення інформаційного простору створює нові можливості для розвитку організованої злочинності, яка поступово наближається до домінування над електронними мережами, що є приводом як до вчинення правопорушень так і до створення злочинних угрупувань, що може втілитися у перехід існуючих груп хакерів і кракерів, які координують свої операції [5, с. 79] до формування кримінальних організацій. Відбувається об'єднання організованої злочинної діяльності з елементами неорганізованої злочинності – правопорушення, які заподіюють значну шкоду, що пов'язані з використанням комп'ютерних технологій чи проти них.

Як свідчить практика, непоодинокими є випадки, коли один із співвиконавців обізнаний про вчинення злочину, створює шкідливі програми, а інший надає інформацію з приводу створення шкідливих програм, не будучи обізнаним про злочинність намірів. На перший погляд такі дії доцільно кваліфікувати як пособництво у вчиненні злочину (ч. 5 ст. 27 КК), проте з огляду на

п. 6 ст. 27 КК, не є співучастю не обіцяне заздалегідь переховування злочинця, знарядь і засобів вчинення злочину, слідів злочину чи предметів, здобутих злочинним шляхом, або придбання чи збут таких предметів. У випадку одночасного, але незапланованого вчинення злочинних дій, наприклад вчинення Dos-атаки кількома особами, внаслідок чого система може вийти з ладу, наявний склад злочину, передбачений ст. 361 КК України, при цьому кожен з учасників може навіть ніколи не бачити інших виконавців, жодним чином не контактувати та навіть не здогадуватися про їх існування, у такому випадку, необхідно кваліфікувати дії кожного з осіб окремо за ст. 361 КК, не застосовуючи при цьому співучасті у вчиненні злочину [6, с. 139].

З огляду на вищезазначене, доцільно розглядати вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку групою осіб за попередньою змовою. Це означає, що в кожного з виконавців злочину повинен бути умисел на попередньо обговорені узгоджені дії, які необхідні для досягнення злочинного результату. До того ж, проміжок часу між змовою і початком здійснення суспільно небезпечних дій не відіграє ключову роль.

Під організованою комп'ютерною злочинністю мається на увазі сукупність комп'ютерних злочинів, що вчиняються у зв'язку зі створенням та діяльністю організованих злочинних угруповань [7]. Відповідно до статті 28 КК України злочин визнається вчиненим організованою групою, якщо у 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 з розподілом функцій учасників групи, спрямованих на досягненні плану, який відомий усім учасникам такої групи [4].

До ознак, притаманних злочинним організаціям науковець М.Й. Коржанський відносить: наявність статуту розробленого і схваленого учасниками групи плану злочинної діяльності та визначення мети групи; наявність організатора (керівника); конспірація (приховування) своєї діяльності; вербування нових членів; наявність загальних правил поведінки, ієрархія стосунків між учасниками групи; наявність матеріальної бази [8, с. 92].

Співучасниками комп'ютерних злочинів є організатор, виконавець, підбурювач та пособник. Організатори злочинних груп у більшості випадках 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» [9, с. 190], не вчиняючи злочинів самотужки. При цьому основною метою організатора такої групи (організації) є утворення стійкого об'єднання осіб для заняття злочинною діяльністю, у даному разі для вчинення комп'ютерних злочинів, забезпечення взаємозв'язку між діями всіх учасників, упорядкування взаємодії його структурних частин.

Дії організатора злочину (злочинів) при 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 приймала участь у вчиненні одного злочину як організатор, а іншого у якості виконавця, посібника чи підбурювача, його дії підлягають окремій кваліфікації у кожному випадку [10].

Характерною ознакою організованої кіберзлочинності є обов'язкова наявність специфічного учасника злочинної групи – хакера (фрікера, крекера тощо) [11, с. 32-33].

Також особливістю злочинів у сфері використання електронно-обчислюваних машин, систем та комп'ютерних мереж, мереж електрозв'язку є використання засобів комунікацій віддаленого доступу, тобто не потребується присутності правопорушників на безпосередньому місці вчинення злочину, адже особливість глобальної мережі – відсутність кордонів. Дедалі частіше хакери об'єднуються у групи, мають ознаки організованих злочинних угруповань. У мережах створюються спеціальні місця для спілкування: форуми, конференції з хакерською тематикою, спеціалізовані сайти. Нерідко відвідування таких місць може бути обмежено та захищено паролями, а зв'язки у злочинних угрупованнях можуть мати як тимчасовий, так і постійний характер з чіткою ієрархією та розподілом ролей у виконанні протиправного посягання [9, с. 190].

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]. Підбурювачем є особа, яка умовлянням, підкупом, погрозою, примусом або іншим чином схилила іншого співучасника до вчинення злочину [4].

Як слушно зазначає Д.О. Ричка, зазвичай організовані злочинні угруповання мають у своїх "штатах" спеціалістів, які займаються розвідкою з використанням найсучасніших технічних засобів для збору 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 у якості засобів або жертв використовують інформаційні системи різних держав світу, з можливістю доступу до національних, у тому числі й спеціально захищених інформаційних ресурсів, що створює нові умови для організованої злочинності –використання мережі Інтернет не тільки для вчинення правопорушень, а й для організації віртуальних банд. Таких учасників доцільно називати пособниками [6, с. 145].

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

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 з 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 [12, с. 56]. З'ясування зазначених питань хоча й не входить до предмету цього дослідження, однак потребує окремого детального вивчення.

Висновки. За результатами дослідження злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку ми дійшли висновку, що їх особливостями є високотехнологічність, латентність, зазвичай груповий характер та високий рівень суспільної небезпечності, що зумовлює складність виявлення та розслідування відповідних злочинів, притягнення усіх учасників угруповання до кримінальної відповідальності.

Під організованою комп'ютерною злочинністю мається на увазі сукупність комп'ютерних злочинів, що вчиняються у зв'язку зі створенням та діяльністю організованих злочинних угруповань. Співучасниками комп'ютерних злочинів є організатор (здебільшого координатори проєктів, під керівництвом яких розробляються плани атак, створюється шкідливе програмне забезпечення, збирається конфіденційна інформація про осіб з метою реалізації на «чорному ринку» тощо), виконавець, підбурювач та пособник. Особливим суб'єктом зазначених злочинів є хакер, який зазвичай є виконавцем злочину. Проміжок часу між змовою і початком вчинення суспільно небезпечних дій у кожного з виконавців комп'ютерного злочину не відіграє ключову роль, водночас повинні бути встановлені умисел на попередньо обговорені узгоджені дії, які необхідні для досягнення злочинного результату.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Полуніна Л.В. Можливості експертизи комп'ютерної техніки і програмних продуктів під час розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин та комп'ютерних мереж. *Проблеми сучасних трансформацій.* 2023. № 7. С. 1-9. DOI: https://doi.org/10.54929/2786-5746-2023-7-01-04
2. Денис С.Р. Практика Верховного Суду щодо кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. С. 1-9. *Академічні візії.* Вип. 12. 2022. DOI: http://dx.doi.org/10.5281/zenodo.7214268
3. Гриців М.І., Антощук В.В. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку. Верховний Суд України: офіційний веб-сайт. URL: https://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257 B7C00499C02 (дата звернення: 06.10.2023).
4. Кримінальний кодекс України: Закон України № 2341-III від 05.04.2001 р. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2341-14/conv#n2491 (дата звернення: 03.10.2023).
5. Борисова Л.В. Суб'єкт (особа) транснаціонального комп'ютерного злочину: криміналістичні й психофізіологічні аспекти. *Актуальні проблеми держави і права*. 2008. Вип. № 44. С. 76-81.
6. Ричка Д.О. Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: дис. … канд. юрид. наук: 12.00.08., Ірпінь, 2019. 212 с.
7. Про організаційно-правові основи боротьби з організованою злочинністю: Закон України від 30.06.1993 № 3341-XII. URL: http://zakon2.rada. gov.ua/laws/show/3341-12. (дата звернення: 03.10.2023).

8. Коржанський М.Й. Кваліфікація злочинів: навч. посіб. Вид. № 2. Київ: Атіка, 2002. 640 с.
9. Міхайліна Т.В. Особливості кваліфікації злочинів із використанням засобів комп'ютерної техніки, що вчиняються групою осіб. *Публічне право.* Вип. № 3. 2011. С. 183-193.
10. Про практику розгляду судами кримінальних справ про злочини, вчинені стійкими злочинними об'єднаннями: Постанова Пленуму ВСУ України від 23.12.2005 № 13 (прийняття 23.12.2005). URL: http://zakon2.rada.gov.ua/laws/show/v0013700-05 (дата звернення: 03.10.2023).
11. 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*. Вип. № 2 (44), 2014. С. 31-37.
12. Злобін Д.Л. Взаємодія операторів мобільного зв'язку з ОВС при розслідуванні комп'ютерних злочинів. *Мат. регіон наук.-практ. сем.* (м. Донецьк, 12 грудня 2008 р.). Донецьк: ДЮІ ЛДУВС, 2009. С. 56–61.