Васильєв Андрій Анатолійович,
кандидат юридичних наук
(*Харківський національний університет внутрішніх справ),*
Пашнєв Дмитро Валентинович,
кандидат юридичних наук, доцент
(*Харківський національний університет внутрішніх справ),*

УДК 343.3

ОСОБЛИВОСТІ КВАЛІФІКАЦІЇ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ЕОМ (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

В статті визначено особливості кримінально-правової характеристики злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Розроблено окремі правила кваліфікації комп'ютерних злочинів.

Ключові слова: комп'ютерний злочин, кваліфікація злочину

Сучасний стан інформатизації суспільства створює нові, раніше не знайомі вітчизняному законодавству про кримінальну відповідальність, форми злочинної поведінки, відкриває нові «горизонти» для професійної злочинності. В поле зору криміналістів, що займаються цією проблематикою, потрапляють не тільки злочини, що безпосередньо пов'язані з комп'ютерами, але й такі злочини як шахрайство з банківськими платіжними картками, злочини у сфері телекомунікацій та інформаційно-телекомунікаційних мереж (шахрайство з оплатою міжнародних телефонних переговорів), незаконне використання банківської мережі електронних платежів, програмне (комп'ютерне) «піратство», шахрайство з використанням ігрових автоматів та багато інших.

У чинному КК України міститься лише один розділ Особливої частини, норми якого прямо пов'язані із використанням комп'ютерних систем – Розділ XVI «Злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Проте, з точки зору кримінально-правової кваліфікації, необхідно чітко встановити конкретну норму КК України, за якою відбудеться юридична оцінка певного діяння, що становить завдання такої кваліфікації. Це обумовлює актуальність наукової розробки питань кваліфікації злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Цього питання торкалися в своїх дослідженнях багато вчених, зокрема: Д. С. Азаров, М. П. Бікмурзін, В. В. Кузнецов, А. А. Музика, Є. В. Лащук, П. І. Орлов, С. О. Орлов, О. Е. Радутний, М. В. Рудик, Н. А. Розенфельд, О. В. Смаглюк, І. О. Юрченко та інші. Але не дивлячись на великий науковий доробок, більшість робіт в цьому напрямку в основному присвячені кримінально-правовій характеристиці комп'ютерних злочинів. Разом з цим, щодо питань кваліфікації діянь за нормами Розділу XVI КК України або за суміж-

ними складами злочинів останнім часом в практиці правоохоронних органів виникає багато проблем, які викликані різноманітністю кримінальної активності в комп'ютерній сфері, елементи якої проникають у все більшу частину охоронюваних кримінальним законом відносин.

Метою даної статті є виявлення особливостей кримінально-правової характеристики злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та розробка рекомендацій щодо кваліфікації діянь за статтями 361–363-1 КК України.

Переважна більшість складів злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (далі – комп'ютерні злочини) є матеріальними, а тому виявляються за наслідками. Отже, під час кваліфікації цих злочинів та їх відмежування від суміжних складів злочинів, необхідно оцінювати розмір та характер заподіяної шкоди з точки зору характеристики її предмету.

Так, предметом більшості комп'ютерних злочинів є комп'ютерна інформація [1] або комп'ютерна система (під якою слід розуміти будь-яку із систем: ЕОМ (комп'ютер), автоматизовану систему, комп'ютерну мережу чи мережу електрозв'язку). Саме злочинний вплив на ці предмети або їх злочинне використання дає підстави визначити наявність об'єкту цих злочинів, тому що вони є невід'ємною частиною охоронюваних розглядуваними нормами суспільних відносин.

Результати злочинного впливу на комп'ютерну інформацію чи комп'ютерну систему слід оцінювати у тісному зв'язку з ознаками об'єктивної сторони, що відносяться до наслідків злочину (витік, втрата, підробка, блокування комп'ютерної інформації, порушення встановленого порядку її маршрутизації (ст. 361), зміна, знищення, блокування комп'ютерної інформації (ст. 362)) тощо.

Зокрема, на практиці зустрічаються випадки кваліфікації внесення до комп'ютерної системи неправдивої інформації особою, яка має права доступу до неї – ст. 362 КК України як несанкціонованої зміни інформації (наприклад, при внесенні нотаріусом у реєстр даних про незаконно оформлену довіреність). В даному випадку фактично відбулося створення інформації в системі, а тому така кваліфікація є недостатньо обґрунтованою.

На випадках такої кваліфікації вчиненого слід зупинитися окремо, оскільки фактично такі діяння не мають ознак жодного складу злочину, що передбачені статтями Розділу 16 Особливої частини КК України. Зокрема, суди кваліфікують такі діяння як втручання в систему – за ст. 361 КК України. Разом з цим, під несанкціонованим втручанням в роботу ЕОМ, їх систем чи комп'ютерних мереж розуміється проникнення до цих машин, їх систем чи мереж і вчинення дій, які змінюють режим роботи машини, її системи чи комп'ютерної мережі, або ж повністю чи частково припиняють їх роботу, без дозволу (згоди) відповідного власника або уповноважених ним осіб, а так само вплив на роботу

АЕОМ за допомогою різних технічних пристроїв, здатних зашкодити роботі машини [2, с. 1036]. Тобто ці дії повинні мати деструктивний характер.

В даному ж випадку особа не вчиняє таких дій – вона створює інформацію, тобто її поведінка не може бути оцінена за ст. 361 КК. І як вже було вказано, інформація не змінюється, не знищується і не блокується, тобто є помилковою і кваліфікація за ст. 362 КК.

На наш погляд, подібні дії, які фактично не містять вказаних в статтях 361–363-1 КК наслідків для системи та комп'ютерної інформації, слід розцінювати як спосіб вчинення іншого злочину і кваліфікувати їх за відповідними статтями інших розділів КК за наявності ознак складу злочину, виходячи зі спрямованості умислу винної особи, наприклад за ч. 3 ст. 190, якщо шляхом такого внесення в систему завідомо неправдивої інформації вчинено заволодіння чужим майном.

При кваліфікації комп'ютерного злочину у будь-якому випадку слід оцінювати розмір завданої шкоди, тому що це має критичне значення для наявності конкретного складу злочину. Зокрема, злочин, передбачений ст. 363 КК України, вважається закінченим, лише якщо заподіяно значну шкоду, а при наявності такого розміру шкоди при вчиненні злочину, передбаченого ст. 361 КК України, кваліфікацію слід проводити за ч. 2 цієї статті. При цьому слід пам'ятати, що шкода у статтях 361–363-1 КК України може полягати в заподіянні матеріальних збитків, які зазвичай є позитивними (позитивна майнова шкода), які оцінюються, виходячи з витрат власника на придбання комп'ютерної інформації, пропорційно зниженню цієї вартості, спричиненої злочином, або виходячи з вартості компонентів комп'ютерної системи (програмних чи технічних), які зазнали негативного злочинного впливу, або виходячи із витрат на відновлення комп'ютерної інформації чи компонентів комп'ютерної системи тощо. Тобто це прямі збитки для потерпілого, підтверджені певними документами. Крім того, збитки від такого злочину можуть мати непряме вираження (опосередковане тощо) та виражатися в упущеній вигоді, що є результатом, наприклад, укладання завідомо невигідної угоди, зниження авторитету, невиконання умов договорів тощо [3, с. 144].

Крім матеріальної шкоди, суспільно небезпечні наслідки при вчиненні комп'ютерного злочину можуть виражатись і в нематеріальних видах шкоди, що зумовлено використанням ЕОМ, систем і комп'ютерних мереж для контролю над складними технологічними процесами, об'єктами та управління ними. Така шкода може виражатися у порушенні нормальної роботи підприємств (установ чи організацій), зупиненні або порушенні складних технологічних процесів, зниження обороноздатності держави, підрив авторитету державних органів, підприємств, установ або організацій, створення загрози або заподіяння шкоди життю чи здоров'ю громадян, порушення безпеки руху транспорту тощо. Так,

у практиці правоохоронних органів можуть виникати випадки, коли в результаті незаконного втручання в роботу автоматизованих систем управління порушувався виробничий процес, створювалася загроза життю багатьох осіб [3, с. 145].

Слід зауважити, що визначити вичерпний перелік можливих наслідків злочину у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку надзвичайно важко, оскільки в кожному випадку ці наслідки залежать насамперед від змісту комп'ютерної інформації, яка зазнала шкоди. Характер шкоди в кожному конкретному злочині, як правило, залежить від тих суспільних відносини, які виступають не основним безпосереднім, а додатковим об'єктом. Це можуть бути відносини в різних сферах життєдіяльності людини, пов'язані з використанням ЕОМ, систем, комп'ютерних мереж і мереж електрозв'язку. Перешкоджаючи інформаційним відносинам, злочинець завдає або загрожує завдати шкоди тим суспільним відносинам, для інтенсифікації яких застосовуються комп'ютерні технології. Отже, велике значення для кваліфікації має визначення додаткового обов'язкового або факультативного об'єкта злочину та шкоди, яку він зазнав.

До того ж, визначення шкоди від злочину у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, особливо непрямої та нематеріальної, утворює велику складність на практиці. Суд досить рідко приймає до уваги розмір шкоди, який не підтверджено документально, не обраховано обґрунтованими методиками, які на даний час для обчислення вартості втраченої комп'ютерної інформації, вартості робіт з відновлення роботи системи та іншої шкоди в сфері комп'ютерних технологій, відсутні. Тому розмір шкоди повинен бути підтверджений всіма можливими документами, які характеризують вартість, яку можна включити у вартість інформації (оплата роботи працівників, які створювали базу даних, вартість покупки частин бази даних для створення якісно нової бази даних тощо), або у втрати потерпілого від неробочої комп'ютерної системи (вартість робіт із відновлення, вартість необхідного для відновлення програмного та технічного забезпечення тощо).

Якщо ж предмет злочинного посягання не має необхідних ознак – інформація не представлена у виді, необхідному для її обробки ЕОМ, чи інформаційна система не є комп'ютерною, – або шкода, яка їй завдана, не відповідає вказаній у відповідних нормах, або шкода цій інформації взагалі не завдана, хоча і були вчинені дії, які входять до об'єктивної сторони певного складу злочину, то мова не може йти про злочин у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

У разі виявлення необхідних ознак суспільно небезпечних наслідків – шкоди яка була заподіяна об'єкту, слід здійснити оцінку такої ознаки об'єктивної сторони як дія (бездіяльність), що призвела до них. Характер діянь, які вчинюються у сфері викорис-

тання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку дозволяє виокремити щонайменше чотири моделі злочинного посягання:

1. Якщо наслідки спричинені діями особи, яка не мала права доступу до комп'ютерної інформації – ці дії мають явні ознаки несанкціонованого втручання в систему, зокрема, здійснені у порушення порядку доступу до інформації або з подоланням засобів захисту інформації тощо. В такому разі, за наявності інших необхідних ознак складу злочину, ці дії слід кваліфікувати за ст. 361 КК України.

2. Якщо наслідки спричинені діями особи, яка мала право доступу до комп'ютерної інформації, але не мала права вчиняти з нею певні дії – змінювати, знищувати, блокувати, перехоплювати або копіювати її. Такі дії слід кваліфікувати за ст. 362 КК України.

3. Якщо наслідки спричинені діями (бездіяльністю) особи, яка відповідає за експлуатацію ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Ці дії чи бездіяльність вчинені у порушення правил експлуатації або порядку чи правил захисту інформації, яка в них оброблюється. В такому випадку подія повинна отримати кримінально-правову оцінку за ст. 363 КК України.

4. Якщо наслідки спричинені будь-якою особою шляхом масового розповсюдження повідомлень електрозв'язку, здійсненого без попередньої згоди адресатів. Очевидно, що такі дії слід кваліфікувати за ст. 363-1 КК України.

Злочини, склади яких відносяться до формальних (статті 361-1 та 361-2 КК України), найчастіше виявляються в ході розслідування інших злочинів, або шляхом отримання правоохоронними органами інформації від заявників, які не є потерпілими від злочину, чи з інших джерел.

В такому випадку для отримання підтвердження ознак певного виду злочину слід провести слідчі (розшукові) дії (огляд, обшук), в необхідних випадках – негласні (контроль за вчиненням злочину). Під час їх проведення необхідно оцінити дії особи, що підозрюється у вчиненні злочину або їх результати на предмет наявності в них ознак об'єктивної сторони певного складу злочину (збут, розповсюдження шкідливих програмних чи технічних засобів або інформації з обмеженим доступом). Крім того, слід звернути увагу і на виявлення необхідних ознак предмета даних злочинів.

Звичайно, кваліфікація діяння не повинна на цьому закінчуватися, адже фактично були оцінені тільки об'єкт та об'єктивна сторона складу злочину. Велика увага повинна приділятися оцінці суб'єктивних ознак: суб'єкта та суб'єктивної сторони складу злочину, оскільки їх невідповідність вимогам КК України виключає кримінальну відповідальність.

Оцінка ознак суб'єкта злочину в сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електро-

зв'язку набуває великого значення також тому, що на сучасному етапі проникнення комп'ютерних технологій в життя суспільства більшість їх користувачів є неповнолітніми, а точніше такими що не досягли віку, з якого може наставати кримінальна відповідальність. Отже слід чітко встановити, що підозрюваний досяг 16 річного віку.

У випадках наявності ознак спеціального суб'єкта (статті 362 та 363 КК України), їх необхідно встановити та оцінити.

Слід мати на увазі, що останнім часом вчені визнають наявність нових видів психічних хвороб, пов'язаних із використанням комп'ютерних технологій [4]. Отже, слід приділити окрему увагу поведінці підозрюваного в ході слідства та відображенням її в механізмі злочинної поведінки (вчиненого діяння) для оцінки осудності цієї особи.

При оцінці суб'єктивної сторони злочину у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку в більшості випадків (статті 361, 361-1, 361-2, 362, 363-1 КК України) необхідно встановити ознаки умислу в діях чи бездіяльності особи. Однак, при цьому слід обмежуватися лише вказаною частиною об'єктивної сторони, адже щодо наслідків у цих складах злочинів може бути і необережна форма вини (матеріальні склади цих злочинів можуть характеризуватися змішаною формою вини). Це стосується тільки тих злочинів, склади яких визнаються матеріальними (ст.ст. 361, 363-1 КК України). Стосовно складу злочину об'єктивна сторона якого описана за допомогою формулювань, які одночасно виступають і діянням, і наслідками (ст. 362 КК України): зміна, знищення або блокування інформації, – форма вини щодо обох цих ознак об'єктивної сторони повинна бути умисною.

Інша ситуація стосується складу злочину, передбаченого ст. 363 ККК України: він може характеризуватися умисною або необережною формою вини щодо діяння, щодо наслідків завжди має місце необережність. В іншому випадку такі дії, за наявності необхідних ознак, можуть кваліфікуватися за ст. 361 чи ст. 362 КК України.

У ході оцінки суб'єктивної сторони злочинів, передбачених ст. 361 та ст. 362 КК України, слід приділяти окрему увагу завідомості – усвідомленню особою щодо якої є підозра несанкціонованості її дій. Оскільки ознаки відсутності в неї такого усвідомлення або відсутність ознак того, що вона мала таке усвідомлення (відсутність підпису про інструктаж, відсутність будь-яких інструкцій з боку власника системи чи інформації тощо), обумовлює і відсутність відповідної форми вини цієї особи – умислу.

Склад злочину ст. 361-1 КК України містить у якості необхідної ознаки суб'єктивної сторони мету вчинення злочину: використання, збут чи розповсюдження предметів злочину. Ця ознака повинна оцінюватися в тісному зв'язку з діянням, яке входить до об'єктивної сторони складу цього злочину – створенням шкідливих програмних чи технічних засобів, призначених для несанкці-

онованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

У разі посягання під час вчинення злочину і на інші суспільні відносини (крім родового об'єкту Розділу 16 КК України), тобто при наявності ознак сукупності злочинів, слід враховувати таке. Ідеальна сукупність злочинів відсутня, якщо вчиненим діянням виконуються злочини, які є обов'язковою (конститутивною) ознакою посягання, передбаченого однією статтею Особливої частини КК [5, с. 224]. Тому слід мати на увазі те, що інформаційні процеси пронизують усі суспільні відносини, і часто діяння, яке передбачено статтею розділу 16 КК України, є способом вчинення іншого, більш тяжкого злочину, а тому не слід кваліфікувати вчинене за сукупністю злочинів. Наприклад, знищення певної надзвичайно важливої для обороноздатності країни комп'ютерної інформації з метою ослаблення держави шляхом несанкціонованого втручання, яке спричинило істотну шкоду, є диверсією, і повинне кваліфікуватися лише за ст. 113 КК України, без додаткової кваліфікації за ч. 2 ст. 361 КК України. Не потребує додаткової кваліфікації і умисне внесення неправдивих відомостей до бази даних Державного реєстру виборців, несанкціоновані дії з інформацією, що міститься у базі даних Державного реєстру виборців, чи інше несанкціоноване втручання у роботу Державного реєстру виборців, вчинене службовою особою, яка має право доступу до цієї інформації, або іншою особою шляхом несанкціонованого доступу до бази даних Державного реєстру виборців (ч. 11 ст. 158 КК України).

Те ж саме стосується і окремих злочинів проти власності. Зокрема, за ч. 3 ст. 190 КК України кваліфікується шахрайство вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки. В даному випадку значення має спрямованість умислу винної особи: особа, маючи умисел на заволодіння чужим майном, наприклад, вносить змини у базу даних комерційного банку щодо розміру депозитного вкладу чи кредиту тощо, тим самим одержуючи майно або утримуючись від необхідності сплати коштів, заподіюючи тим самим шкоду банку. При цьому незаконні операції з використанням електронно-обчислювальної техніки виступають способом вчинення обману при шахрайстві.

В інших випадках, коли своїми діями чи бездіяльністю особа порушила і інформаційні відносини, забезпечені комп'ютерними технологіями, і будь-які інші, кваліфікація повинна відбуватися за правилами сукупності злочинів.

В ході оцінки події, яка не містить достатніх ознак складу злочину, хоч в ній і фігурували ЕОМ (комп'ютер), система, комп'ютерна мережа або мережа електрозв'язку, слід мати на увазі, що вона може бути кваліфікована як незакінчений злочин або співучасть у злочині. Зокрема, досить розповсюдженими є діяння, передбачені ст. 6 Конвенції про кіберзлочинність [6], вони можуть розглядатися як умисний продаж, розповсюдження або надання для використання іншим чином комп'ютерних паро-

лів, кодів доступу або подібних даних з метою подальшого вчинення злочинів, передбачених статтями розділу 16 КК України і являти собою пособництво у вчиненні відповідних злочинів (необхідним є посилання на ч. 5 ст. 27 КК України); володіння шкідливими засобами з метою подальшого вчинення злочинів необхідно, відповідно до національного законодавства, вважати готуванням до відповідних злочинів (необхідним є посилання на ч. 1 ст. 14 КК України).

Таким чином, під час кваліфікації, використовуючи виявлені в цій статті особливості складів комп'ютерних злочинів, доцільно дотримуватися певних правил:

1) кваліфікацію комп'ютерних злочинів, склади яких є матеріальними, слід розпочинати з оцінки їх наслідків у розрізі предмета злочину, далі оцінити зміст та характер діяння, причинний зв'язок між діянням винної особи та наслідками, ознаки цієї особи, і залежно від цього обрати відповідну норму КК України;

2) кваліфікацію комп'ютерних злочинів, склади яких є формальними, слід розпочинати із встановлення відповідних ознак діяння та предмету злочину;

3) незалежно від складу злочину слід оцінити суб'єктивні ознаки з огляду на знижений вік комп'ютерних користувачів та вплив комп'ютерних технологій на психіку людини;

4) при оцінці сукупності злочинів слід звертати увагу на велику ймовірність поглинення діяння, яке містить ознаки комп'ютерного злочину, складом іншого злочину;

5) при оцінці діянь в комп'ютерній сфері, які прямо не передбачені КК України, необхідно спробувати застосувати до них правила кваліфікації незакінченого злочину або співучасті у злочині.

Звичайно, в рамках однієї статті неможливо окреслити всі особливості кваліфікації певного виду злочинів, але з огляду на майже відсутність праць у даному напрямі, сподіваємося, що наші висновки сприятимуть активізації наукової дискусії та подальшим пошукам, спрямованим на вирішення практичних питань кваліфікації комп'ютерних злочинів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Пашнєв Д. В. Властивості комп'ютерної інформації як предмету злочину / Д. В. Пашнєв // Вісник Кримінологічної асоціації України : збірник наукових праць [Редкол. Л. М. Давиденко, Т. А. Денисова, О. М. Джужа та ін.]. – № 1. – Х. : ХНУВС, 2012. – 308 с. – С. 115-125.

2. Науково-практичний коментар Кримінального кодексу України / За ред. М. І. Мельника, М. І. Хавронюка. – 7-ме вид., переробл. та допов. – К. : Юридична думка, 2010. – 1288 с.

3. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.]. – К. : Видавничий дім «Скіф», 2012. – 728 с.

4. Чорна В. В. Комп'ютер і комп'ютерні ігри. За і проти // Гігієна населених місць. – 2008. – № 52. – С. 338–342.

5. Навроцький В. О. Основи кримінально-правової кваліфікації : навч. посіб. / В. О. Навроцький. – 2-ге вид. – К. : Юрінком Інтер, 2009. – 512 с.

6. Конвенція про кіберзлочинність від 23.11.2001 р. [Електронний документ] / Верховна Рада України : Законодавство. – 25.08.2012 р. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/994_575.

В статье выявлены особенности криминально-правовой характеристики преступлений в сфере использования ЭВМ (компьютеров), систем, компьютерных сетей и сетей электросвязи. Разработаны отдельные правила квалификации компьютерных преступлений.

Ключевые слова: *компьютерное преступление, квалификация преступления*

The article reveals some features of criminal and legal characteristics of the crimes in the sphere of usage of ECM (computers), systems, computer networks and telecommunication networks. Separate rules for the qualification of computer crimes are worked out.

Key words: *computer crime, the qualification of the crime*

Стаття надійшла до редакції 05.10.2013