ISSN 1995-6134

УДК 343.3/.7
Д.В. ПАШНЄВ, канд. юрид. наук, доц.,
Харківський національний університет внутрішніх справ
ORCID: http://orcid.org/0000-0001-8693-3802
О.О. АВДЄЄВ, канд. юрид. наук,
Харківський національний університет внутрішніх справ
ORCID: http://orcid.org/0000-0003-4203-8165

КВАЛІФІКАЦІЯ КІБЕРЗЛОЧИНІВ У ВИПАДКАХ ІДЕАЛЬНОЇ СУКУПНОСТІ ЗЛОЧИНІВ

Ключові слова: *кіберзлочин, кримінально-правова кваліфікація, ідеальна сукупність злочинів*

Сучасний стан інформатизації суспільства створює нові, раніше не знайомі вітчизняному законодавству про кримінальну відповідальність, форми злочинної поведінки, відкриває нові «горизонти» для професійної злочинності. Комп'ютерні системи містять в собі новітні, більш досконалі можливості для невідомих раніше правопорушень, а також для скоєння, так би мовити, традиційних злочинів, але нетрадиційними засобами. В поле зору криміналістів потрапляють не тільки злочини, що безпосередньо і тільки пов'язані із завданням шкоди відносинам в сфері використання комп'ютерних систем, але й суспільно небезпечні посягання на інші, традиційні об'єкти: національну безпеку, власність, громадську безпеку, громадський порядок та моральність, інші не менш важливі суспільні відносини, і навіть життя та здоров'я особи [1].

В ході протидії кіберзлочинам, як називають цей новий вид правопорушень, центральне місце займає їх кримінально-правова кваліфікація, як процес та результат юридичної оцінки певного діяння, завданням якої фактично є чітке встановлення конкретних норм Кримінального Кодексу України (далі – КК), якими це діяння передбачене. З причин новизни цього явища та широкого розповсюдження в різних сферах кримінально-правової охорони разом із проникненням до них комп'ютерних технологій, актуальність наукової розробки питань кваліфікації кіберзлочинів ще довго буде залишатися на високому рівні.

Кримінально-правових питань протидії кіберзлочинності 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 окремих кіберзлочинів. Разом із тим, більшість питань кваліфікації цих діянь, в процесі якої на практиці в працівників правоохоронних та судових органів виникає багато проблем, ще потребують свого наукового вирішення. Особливо це стосується випадків вчинення кіберзлочинів, що посягають на декілька об'єктів, охоронюваних кримінальним законом.

Найчастіше помилки кваліфікації зустрічаються при кваліфікації одного діяння, яке, на перший погляд, містить ознаки декількох складів злочинів. Отже, основною проблемою, вирішення якої впливає на правильність кваліфікації кіберзлочинів, є визначення наявності або відсутності у вчиненому ідеальної сукупності злочинів. Тому метою статті є виявлення особливостей застосування правил кваліфікації ідеальної сукупності злочинів в ході кримінально-правової кваліфікації кіберзлочинів.

Безперечно, вірним є початок дослідження явища із правильного його визначення. Ми переконані, що визначення кіберзлочину необхідно давати виходячи з двох частин, з яких цей термін складається: «злочин» та «кібер». При цьому, слід використовувати законодавче визначення поняття злочину та термін «інформаційно-телекомунікаційна система»

ISSN 1995-6134

(далі – ІТС) відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», оскільки ми вважаємо, що терміни КК – електронно-обчислювальні машини (комп'ютери), їх системи, комп'ютерні мережі, мережі електрозв'язку – не охоплюють усі випадки сучасного та майбутнього застосування комп'ютерних технологій, хоча цей вислів імає великий обсяг.

Отже, кіберзлочин – це передбачене КК суспільно небезпечне винне діяння, вчинене суб'єктом злочину з використанням ІТС.

Навіть поверхневий аналіз практики протидії цьому явищу дає підстави для висновку, що в ході вчинення кіберзлочину шкода може завдаватися в трьох варіантах: 1) суспільним відносинам, які виникають в ході забезпечення за допомогою ІТС життєдіяльності людини, суспільства, держави; 2) традиційним суспільним відносинам, охоронюваним кримінальним законом, які забезпечуються за допомогою ІТС, цілеспрямований шкідливий вплив на які використовується для завдання шкоди цим відносинам; 3) традиційним суспільним відносинам, охоронюваним кримінальним законом, для нанесення шкоди яким використовуються ІТС, які, в свою чергу, не зазнають при цьому шкоди.

Перша група відносин охороняється Розділом 16 Особливої Частини КК (Злочини в сфері використання ЕОМ (комп'ютерів), їх систем, комп'ютерних мереж, мереж електрозв'язку). Ці відносини є частиною другої та третьої групи відносин, але в другій групі вони зазнають шкоди разом із традиційними відносинами кримінально-правової охорони, а в третій – ні.

Ідеальною сукупністю злочинів вважається два або більше злочини вчинені одним діянням. Відповідно до вказаних нами груп відносин, що зазнають шкоди при вчиненні такого діяння у випадку вчинення кіберзлочину, можна виділити три групи цих злочинів, що будуть мати свої особливості кваліфікації відповідно до діючого КК: 1) злочини в сфері використання ЕОМ (комп'ютерів), їх систем, комп'ютерних мереж, мереж електрозв'язку (Розділ 16 Особливої Частини КК); 2) злочини, що кваліфікуються за статтями КК відповідно до об'єкту посягання з додатковим посиланням на статті Розділу 16 Особливої Частини КК; 3) злочини, що кваліфікуються за статтями КК відповідно до об'єкту посягання без додаткового посилання на статті Розділу 16 Особливої Частини КК.

Тобто діяння з першої та третьої групи є одиничними злочинами, а з другої – ідеальною сукупністю злочинів. Але в практиці застосування норм КК в протидії кіберзлочинам діяння, що відносяться до різних із вказаних намигруп, часто плутаються. Найчастіше, злочини другої групи кваліфікуються тільки за однією статтею,і навпаки, злочини першої чи третьої групи кваліфікуються за декількома статтями, хоча не потребують додаткової кваліфікації. При цьому стаття, яка застосовується при кваліфікації другої групи злочинів, або із Розділу 16 Особливої Частини КК, або інша – відповідно до безпосереднього об'єкту посягання. Очевидно, що в обох цих випадках частина злочину кваліфікацією не охоплюється, що порушує принципи повноти та точності кваліфікації, а у разі кваліфікації одного діяння, яке містить один склад злочину, за двома статтями порушується ще й принцип заборони подвійного інкримінування.

Про наявність таких фактів свідчить узагальнення судової практики. Зокрема, велика частка кіберзлочинів припадає на випадки, коли посягання в сфері використання ІТС здійснюється з корисливих мотивів з метою викрадення чи заволодіння чужим майном із заподіянням потерпілим матеріальної шкоди і є способом вчинення таких злочинів проти власності, як шахрайство (ст.190 КК) або привласнення чи заволодіння майном шляхом зловживання службовим становищем (ст.191 КК). У більшості випадків суди кваліфікують такі дії за сукупністю злочинів: за статтею

ISSN 1995-6134

Розділу 16 Особливої Частини КК і тією статтею, в якій передбачено відповідальність за конкретний злочин проти власності, способом здійснення якого було використання ІТС.

Наприклад, Печерський районний суд м. Києва визнав М. винним у тому, що він, працюючи провідним інженером відділу пластикових карток акціонерного комерційного «Промислово-фінансового банку», як службова особа, що виконує адміністративно-господарські функції, зловживаючи своїм службовим становищем, маючи доступ до бази даних про клієнтів та їхні рахунки, що містилась у його робочому комп'ютері, діючи з метою заволодіння грошовими коштами, виконав операцію з персоналізації сторонньої картки, скопіювавши на неї інформацію одного з клієнтів банку. З використанням картки-дубліката та банкоматів М. зняв і привласнив готівкою з рахунку клієнта грошові кошти на загальну суму 65 тис. 900 грн. Зазначені дії М. суд кваліфікував за ч.4 ст.191 КК як заволодіння чужим майном шляхом зловживання службовим становищем, вчинене у великих розмірах. Крім того, суд кваліфікував дії М. ще й за сукупністю з ч.3 ст.362 КК, оскільки М., будучи особою, яка мала право доступу до інформації, що оброблялася на комп'ютерах та зберігалася на носіях, несанкціоновано її скопіював, що призвело до витоку інформації і заподіяло значну шкоду.

Проте в деяких випадках суди кваліфікують зазначені дії лише за статтями Розділу 16 Особливої Частини КК.

Так, Красногвардійський районний суд м. Дніпропетровська визнав Є. винним за ч.1 ст.361 КК і призначив йому відповідне покарання. З матеріалів справи вбачається, що Є., діючи з корисливих мотивів, за допомогою спеціальних комп'ютерних програм створив дублікат-макет сайту компанії, яка спільно із ЗАТ КБ «ПриватБанк» надавала послуги з прискореного перерахування платежів за комунальні послуги і мобільний зв'язок через мережу Інтернет. У результаті такої діяльності Є. протягом певного часу викрадав грошові кошти з рахунків клієнтів ЗАТ КБ «ПриватБанк» [2].

Автори узагальнення, з якого взяті ці приклади, вважають що в останньому випадку, оскільки Є. шляхом обману неодноразово заволодівав грошовими коштами за допомогою незаконних операцій з використанням ЕОМ, а втручання в роботу ЕОМ є способом вчинення злочину проти власності, то в цьому випадку зазначені дії потребують додаткової кваліфікації ще й за ст.190 КК (шахрайство). Вважаємо, що тут дійсно наявна сукупність злочинів, але вона вже врахована в КК в ч.3 ст.190, отже потрібна кваліфікація за цією нормою без додаткових посилань на норми КК.

Питання кваліфікації за ознаками шахрайства шляхом незаконних операцій з використанням електронно-обчислювальної техніки також є проблемним і остаточно не вирішеним для науки кримінального права [3–5], але більшість його аспектів потребують окремого дослідження, а тому зупинимося в цьому дослідженні лише на наявності в цьому випадку ідеальної сукупності злочинів, яка вже врахована законодавцем.

На відсутність необхідності додаткової кваліфікації в цьому випадку чітко вказував Пленум Верховного Суду України в часи свого існування: «...шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки, має кваліфікуватися за частиною третьою статті 190 КК і додаткової кваліфікації не потребує».Але перед цим Пленум чітко вказує:«Якщо обман чи зловживання довірою при шахрайстві полягають у вчиненні іншого злочину, дії винної особи належить кваліфікувати за відповідною частиною статті 190 КК і статтею, що передбачає відповідальність за цей злочин» [6].

У цих розмірковуваннях ми приходимо до однієї із загальних проблем кримінально-правової кваліфікації: питання кваліфікації ідеальної сукупності злочинів, а саме поглинання одного злочину іншим, який був його

ISSN 1995-6134

частиною. Ця проблема досі потребує вирішення вченими, про що свідчить недавнє дослідження Т.І. Созанського [7].

Проте, дослідники кримінально-правових питань протидії кіберзлочинності сприймають цю проблему без критичного аналізу, зауважуючи, що в деяких випадках, умисне заподіяння істотної шкоди в результаті комп'ютерного злочину може фактично представляти собою склад іншого злочину. Наприклад, для них цілком очевидно, що знищення певної надзвичайно важливої для обороноздатності країни комп'ютерної інформації з метою ослаблення держави не представляє собою несанкціоноване втручання, яке спричинило істотну шкоду (ч.2 ст.361 КК), а є нічим іншим як диверсією (ст.113 КК) [8, с.146].

М.Й. Коржанський, виводячи правила кваліфікації за сукупністю на підставі досягнутих ним висновків, вивів загальне правило кваліфікації злочинів за сукупністю: якщо вчинене є посяганням на різні безпосередні об'єкти кримінально-правової охорони, то його належить кваліфікувати як сукупність злочинів [9, с.60]. В наведеному ж вище випадку безпосередні об'єкти різні, отже підстав кваліфікувати описаний злочин як одиничний бути не повинно.

Але той же М.Й. Коржанський уточнює своє правило стосовно злочинів, які мають додаткові об'єкти посягання: діяння, при якому заподіяння шкоди додатковому безпосередньому об'єктові посягання є способом, складовою частиною заподіяння шкоди головному безпосередньому об'єктові, кваліфікується як один злочин;діяння, при вчиненні якого шкода додатковому об'єктові заподіюється факультативно, кваліфікується за сукупністю злочинів [10, с.97].

Т.І. Созанський, на наш погляд, формулює це правило більш зрозуміло: «Якщо ці об'єкти співвідносяться як основний і додатковий, то діяння кваліфікується як одиничний злочин, якщо ж обидва (чи більше) об'єкти є основними, то діяння утворює ідеальну сукупність злочинів». Але далі він вказує, що практично визначити, коли об'єкт є додатковим, а коли він переходить у основний,доволі складно [11]. Це набуває критичного значення при оцінці кіберзлочину, адже з точки зору отримання шкоди відділити відносини в сфері використання ІТС від відносин, автоматизацію яких вони забезпечують, в більшості випадків дуже складно.

Т.І. Созанський пропонує, як один із варіантів вирішення цього питання, визначати суспільну небезпечність посягань на відносини, які охороняються цими об'єктами. Якщо суспільна небезпечність відносин,що охороняються додатковим об'єктом, є більшою, ніж основного об'єкта, то діянняутворює ідеальну сукупність [11].

У практичну площину цю рекомендацію перевів Пленум Верховного Суду України у постанові, яка стосується судової практики застосування норм про множинність злочинів [12]. У п.11 цієї постанови вказано: «Якщо у складі злочину передбачене діяння, яке у поєднанні з іншими обставинами завжди утворює склад іншого злочину, то питання про його кримінально-правову оцінку необхідно вирішувати з урахуванням того,наскільки охоплюється складом цього злочину таке діяння,а також з урахуванням змісту санкцій відповідних статей (частин статей) Особливої частини КК. У випадках,коли складом певного злочину охоплюється вчинене одночасно з цим злочином відповідне діянняі санкцією статті (частини статті) Особливої частини КК встановлене за цей злочин більш суворе максимальне основне покарання,ніж за відповідне діяння,таке діяння не утворює сукупності злочинів і окремої кваліфікації не потребує».

В даному випадку Пленум Верховного Суду України фактично суперечить своїм же рекомендаціям щодо кваліфікації за ст.190, наведеним вище. Але при цьому, визнавши свою помилку, він підтримав висловлену вище думку науковців, яка, на наш погляд, є

ISSN 1995-6134

найбільш вірним виходом із цієї складної ситуації.

Таким чином, слід визнати за правило кваліфікації кіберзлочинів, які через посягання на відносини в сфері використання ІТС посягають на інші «традиційні» відносини, які забезпечуються цими ІТС, наступне: у разі, коли складом певного злочину охоплюється вчинене одночасно з цим злочином діяння, передбачене статтею Розділу 16 Особливої Частини КК, і санкцією статті (частини статті) Особливої частини КК встановлене за цей злочин більш суворе максимальне основне покарання, ніж за діяння, передбачене статтею Розділу 16 Особливої Частини КК, таке діяння не утворює сукупності злочинів і окремої кваліфікації не потребує.

ЛІТЕРАТУРА

1. Киллер из компьютера (беседа с заместителем начальника управления «К» ГУВД Самарской области Павлом Шмелевым) / Валерий Ерофеев [Електронний ресурс]. – Режим доступу: http://историческая-самара.рф/каталог/самара-криминальная/случаи-и-факты/киллер-из-компьютера.html.

2. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку / М. І. Грицівий, В. В. Антощук [Електронний ресурс]. – Режим доступу: http://www.scourt.gov.ua/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02.

3. Дудоров О. О. Проблеми кваліфікації шахрайства / О. О. Дудоров // Інтернет-конференція Івано-Франківського обласного осередку ВГО «Асоціація кримінального права» (11-16 березня 2014 р.) [Електронний ресурс]. – Режим доступу: http://law-dep.pu.if.ua/conference2014/articles/dudorov.pdf.

4. Карчевський М. В. Особливості кваліфікації шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки / М. В. Карчевський // Науковий вісник Львівськ. держ. ун-ту внутр. справ. Серія «юридична». – 2014. – Вип. 1. – С. 272–281.

5. Тарасова О. В. Удосконалення законодавства щодо кримінальної відповідальності за шахрайство, учинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки (ч.3 ст.190 Кримінального Кодексу України) / О. В. Тарасова // Актуальні проблеми держави і права. – 2014. – Вип. 72. – С. 481–488.

6. Постанова Пленуму Верховного Суду України «Про судову практику у справах про злочини проти власності» : від 06.11.2009 р., № 10 [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/v0010700-09.

7. Созанський Т. І. Кваліфікація сукупності злочинів : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 / Т. І. Созанський ; Львівськ. держ. ун-т внутр. справ. – Л., 2009. – 20 с.

8. 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.

9. Коржанський М. Й. Кваліфікація злочинів : навч. посіб. / М. Й. Коржанський. – Вид. 2-ге. – К. : Атіка, 2002. – 640 с.

10. Коржанский Н. И. Объект посягательства и квалификация преступления : учеб. пособие / Н. И. Коржанский ; М-во внутр. дел СССР, Высш. следств. школа. – Волгоград : Высш. следств. школа, 1976. – 120 с.

11. Созанський Т. І. Кваліфікація злочинів, передбачених різними статтями КК України / Т. І. Созанський // Європейські

ISSN 1995-6134

перспективи. – 2012. – № 2 (Ч. 1). – С. 131–136.

12. Постанова Пленуму Верховного Суду України «Про практику застосування судами законодавства про повторність, сукупність і рецидив злочинів та їх правові наслідки» : від 04.06.2010 р., №7 // Вісник Верховного Суду України. – 2010. – № 7 (119).

Пашнєв Д. В. Кваліфікація кіберзлочинів у випадках ідеальної сукупності злочинів / Д. В. Пашнєв, О. О. Авдєєв // Форум права. – 2016. – № 4. – С. 258–263 [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/j-pdf/FP_index.htm_2016_4_42.pdf

Виявлено, що основною проблемою при кваліфікації кіберзлочинів, що вчинені одним діянням, але мають ознаки різних складів злочинів, є оцінка цього діяння як одиничного злочину або ідеальної сукупності. Надано спосіб вирішення цієї проблеми через порівняння тяжкості злочинів, ознаки яких містить діяння, що кваліфікується.

***

Пашнев Д.В., Авдеев А.А. Квалификация киберпреступлений в случаях идеальной совокупности преступлений

Выявлено, что основной проблемой при квалификации киберпреступлений, совершенных одним действием, но имеющих признаки различных составов преступлений, является оценка этого деяния как единичного преступления или идеальной совокупности. Предложен способ решения этой проблемы через сравнение тяжести преступлений, признаки которых содержит деяние, которое подлежит квалификации.

***

Pashnev D.V., Avdeev A.A. Qualification of the Cybercrime in Case the Ideal Set of Crimes

It is found that the main problem in qualification of the cybercrime committed in one action, but had signs of various offenses, it is to assess that this action is a single crime or an ideal set of crimes. It is suggested the way to solve this problem by comparing the heinousness of the offences, the symptoms of which includes an action that is subject to qualification.