УДК 343.3/.7

Васильєв Андрій Анатолійович,
кандидат юридичних наук, доцент
(Харківський національний університет внутрішніх справ)

Пашнєв Дмитро Валентинович,
кандидат юридичних наук, доцент
(Харківський національний університет внутрішніх справ)

ОСОБЛИВОСТІ КВАЛІФІКАЦІЇ КІБЕРЗЛОЧИНІВ ПРОТИ ВЛАСНОСТІ

У статті встановлено особливості застосування окремих статей Розділу VI Особливої частини Кримінального кодексу України при кваліфікації злочинів проти власності, що вчиняються з використанням інформаційно-телекомунікаційних систем. З'ясовано випадки, в яких необхідна додаткова кваліфікація таких злочинів за статтями Розділу XVI Особливої частини Кримінального кодексу України.

Ключові слова: злочини проти власності, інформаційно-телекомунікаційна система, кваліфікація, кіберзлочин, кримінально-правова оцінка.

Постановка проблеми. Сучасний стан інформатизації суспільства створює нові, раніше не знайомі вітчизняному законодавству про кримінальну відповідальність форми злочинної поведінки, відкриває нові «горизонти» для корисливої професійної і організованої злочинності. Комп'ютерні системи та мережі містять у собі новітні, більш досконалі можливості для невідомих раніше правопорушень, а також для скоєння, так би мовити, традиційних злочинів, але нетрадиційними засобами. Усе частіше в поле зору криміналістів потрапляють не тільки злочини, що безпосередньо і тільки пов'язані із заподіянням шкоди відносинам у сфері використання комп'ютерних систем чи мереж, 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].

У ході протидії кіберзлочинам, як називають цей новий вид правопорушень, центральне місце посідає 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 в якості злочину. З причин новизни цього явища та глибокого проникнення комп'ютерних технологій у різні сфери суспільних відносин, поставлених під охорону законом про кримінальну відповідальність, актуальність наукової розробки питань кваліфікації кіберзлочинів ще довго буде залишатися на високому рівні.

Аналіз останніх досліджень і публікацій. Кримінально-правових питань протидії кіберзлочинності торкалися у 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 у цьому напрямі в основному

присвячені кримінально-правовій характеристиці окремих кіберзлочинів. Водночас більшість питань кваліфікації цих діянь, у процесі якої на практиці у працівників правоохоронних та судових органів виникає багато проблем, потребують свого наукового вирішення. Особливо це стосується випадків вчинення кіберзлочинів, які одночасно посягають на декілька об'єктів, поставлених під охорону закону про кримінальну відповідальність.

Найбільш розповсюдженим різновидом названих злочинів є, звичайно, корисливі посягання, а саме злочини проти власності. Питання кваліфікації таких злочинів викликають масу проблем на практиці, кримінально-правова оцінка цих діянь здійснюється по-різному для однакових випадків, допускаються помилки при кваліфікації, зокрема, врахування сукупності злочинів у випадках її відсутності і, навпаки, неврахування при її наявності, невірна правова оцінка способу вчинення злочину, а отже і невірний вибір норми Розділу VI КК тощо. У результаті порушуються принципи кримінально-правової кваліфікації: стабільність, повнота, точність, індивідуальність кваліфікації, недопустимість подвійного інкримінування тощо.

Мета роботи. Здійснення кримінально-правової оцінки найбільш поширених випадків вчинення злочинів проти власності, у яких у якості способу чи засобу їх вчинення є інформаційно-телекомунікаційна система, а також вироблення загальних правил кваліфікації кіберзлочинів проти власності.

Виклад основного матеріалу дослідження. Механізм вчинення досліджуваних злочинів, як правило, полягає в тому, що інформаційно-телекомунікаційна система (далі – ІТС) [2], яка утворена або існує на підприємстві, в установі, організації чи у фізичної особи, як правило, використовується злочинцем для здійснення незаконного переказу коштів чи незаконного заволодіння чужим майном тощо, при чому одночасно може вчинятися діяння, яке містить ознаки складу злочину, передбаченого Розділом XVI Особливої Частини КК (далі – Розділ XVI КК).

Нормою, на яку перш за все звертається увага практиків при кваліфікації таких діянь, є ч. 3 ст. 190 КК – шахрайство, вчинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки. Дослідженням проблем її застосування присвячено багато праць [3–6], проте їх кількість не зменшується. Цей комплекс проблем потребує ґрунтовного дослідження, в нашому обмеженому дослідженні ми лише констатуємо їх наявність та висловимо свою точку зору.

Заволодіння чужим майном слід кваліфікувати за ч. 3 ст. 190 КК лише за наявності необхідних умов. Перш за все слід ураховувати, що за змістом обману чи зловживання довірою, як способів вчинення шахрайства, вони можуть бути спрямовані тільки на людину. Це витікає із необхідної ознаки шахрайства – добровільної передачі майна законним володільцем злочинцю [7, с. 201]. Таким чином, обманути чи використати довіру інформаційно-телекомунікаційної системи неможливо. А тому випадки, в яких без безпосередньої участі людини, а лише шляхом надання неправдивої чи підробленої інформації технічному чи програмному засобу (банкомату, платіжній системі, терміналу тощо) відбувається заволодіння майном, слід кваліфікувати як таємне викрадення чужого майна – крадіжку (ст. 185). Таку позицію вказано і в абз. 2 п. 17 постанови Пленуму Верховного Суду України від 06.11.2009 № 10 «Про судову практику у справах про злочини проти власності» (далі – Постанова): «Обман (повідомлення потерпілому неправдивих відомостей або приховування певних обставин) чи зловживання довірою (недобросовісне використання довіри потерпілого) при шахрайстві застосовуються винною особою з метою викликати у потерпілого впевненість у вигідності чи обов'язковості передачі їй майна або права на нього» [8].

Указане діяння слід вважати викраденням, адже воно цілком підпадає під таємний спосіб, коли особа заволодіває чужим майном: за відсутності власника або інших осіб; у присутності власника або інших осіб, але непомітно для них; у присутності власника або інших осіб, які, однак, не усвідомлюють самого факту викрадення і не можуть дати таким діям належної оцінки внаслідок певних обставин (малолітства, фізичних і психічних недо-

ліків, стану алкогольного сп'яніння, помилки); у присутності осіб, які схвалюють або ставляться байдуже до факту вчинення крадіжки винним, і останній це усвідомлює [9, с. 256].

З іншого боку, у таких випадках комп'ютерна система виконує функції посередника між законним володільцем (власником) майна та злочинцем. Законний володілець (власник) делегує системі свої повноваження по передачі майна іншій особі (особам) на підставі перевірки певних ознак: пред'явлення банківської картки або надання її реквізитів та перевірочної інформації тощо. Указана ситуація, зокрема, аналогічна випадку, коли законний володілець (власник) передає майно набувачу через посередника, який повинен розпізнати його за певними ознаками, але зловмисник, заздалегідь знаючи про такий спосіб передачі майна, створює умови для вчинення злочину: маскується під законного набувача, якому посередник під впливом такого обману передає майно. Описана подія, вочевидь, буде кваліфікована як шахрайство, оскільки обману піддається людина – посередник. Але чим останній відрізняється від технічного засобу, який також виконує функцію посередника між законним володільцем (власником) та особою, яка за певними ознаками повинна отримати майно?

На наш погляд, у нових умовах життя, багато аспектів якого опосередковуються комп'ютерними технологіями, «введення в оману або обман» технічних засобів та пристроїв, в яких вони втілюються і реалізують інформаційні процеси суспільних відносин, повинно розглядатися як обман людини, що використовує ці засоби. Однак, безумовно, ця пропозиція ще повинна пройти перевірку часом та отримати наукове обґрунтування в ході спеціальних досліджень.

Прикладом правильної кваліфікації за ч. 3 ст. 190 КК є застосування її при кримінально-правовій оцінці злочинного використання недоліків у роботі касового терміналу, який, якщо після друку чеку швидко висмикнути дріт живлення, відміняє платіжну операцію із нарахування грошей на телефонний рахунок [10]. У даному випадку шляхом несанкціонованого втручання в роботу терміналу (незаконні операції з використанням ЕОТ за змістом ч. 3 ст. 190 КК) отримується чек, який створює ілюзію переведення коштів на рахунок – обман клієнта, під впливом чого він «добровільно» віддає свої гроші (шахрайство).

Надаючи кримінально-правову оцінку вчиненому, слід правильно розуміти зміст терміну «незаконність» операцій з використанням електронно-обчислювальної техніки (далі – ЕОТ). На практиці допускається звужене чи, навпаки, розширене тлумачення цього терміну. Перше тлумачення включає в себе лише діяння, які передбачені статтями розділу XVI КК, і цей підхід передбачає розгляд ч. 3 ст. 190 КК як випадку законодавчо закріпленої ідеальної сукупності злочинів, де спосіб вчинення одного злочину включає (поглинає) вчинення іншого злочину. Друге – дозволяє розглядати будь-які дії з використанням електронно-обчислювальної техніки, що суперечать законодавству, в якості способу вчинення цього злочину.

Класичним прикладом застосування обох цих підходів на практиці є кваліфікація заволодінь чужим майном шляхом публікації фіктивних об'яв про продаж товарів на спеціалізованих сайтах.

Наприклад, реалізуючи свій умисел, спрямований на заволодіння чужим майном, підсудний на сайті Інтернет-аукціону «www.Aukro.ua» розмістив 6 оголошень про продаж мобільних телефонів моделей «Sony Ericsson» та «HTC» за цінами від 1030 грн. до 3580 грн. за один екземпляр. При цьому підсудний для забезпечення можливості отримання перерахованих замовниками товару грошей вказав дійсний номер банківської карти «ПриватБанку». Після надходження замовлень на придбання товару та його передплати підсудний, створюючи видимість виконання своїх зобов'язань перед замовниками, у кожного із них брав адреси відправки, чим уводив потерпілих в оману, оскільки не мав наміру відправляти їм замовлений товар [11].

Указаний випадок був кваліфікований судом за ч. 3 ст. 190 КК. Проте зустрічається достатня кількість вироків, у яких застосовуються й інші частини ст. 190 КК [12]. І в тих, і

в інших випадках суди не можна звинувачувати в неправильному застосуванні норм матеріального права, адже вони детально обґрунтовують або незаконність операцій, або її відсутність: у першому випадку – незаконністю розміщення неправдивої інформації про продаж товару, а в другому – відсутністю вчинення діяння, передбаченого однією зі статей Розділу XVI КК, якими обмежуються незаконні операції з використанням ЕОТ за змістом ч. 3 ст. 190 КК.

На наш погляд, більш прийнятним є розширене тлумачення незаконних операцій з використанням ЕОТ за ч. 3 ст. 190 КК. Такий висновок можна зробити із буквального тлумачення положень КК, у частині наявності й інших випадків законодавчого закріплення сукупності злочинів, передбачених Розділом XVI КК, та інших злочинів, наприклад, у ст. 158 КК передбачено відповідальність за несанкціоноване втручання у роботу бази даних Державного реєстру виборців (діяння органічно поєднано зі способом – використанням ЕОТ і являє собою спеціальну норму). Отже, якщо б законодавець вважав би за необхідне обмежити незаконні операції з використанням ЕОТ у ч. 3 ст. 190 КК тільки діяннями Розділу XVI КК, то доцільно було б використати термінологію вказаного розділу. Очевидно, що термін «електронно-обчислювальна техніка» нерівнозначний терміну «електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку». Логічним є висновок, що до вказаних незаконних операцій повинні відноситися будь-які дії з використанням будь-якої ЕОТ, які суперечать положенням чинного законодавства.

За наявності необхідних умов та у випадку заподіяння значної майнової шкоди, кіберзлочини слід кваліфікувати і за ст. 192 КК як спричинення значної майнової шкоди шляхом обману без ознак шахрайства. При цьому слід враховувати, що відповідно до цієї статті незаконні дії майнового характеру вчиняються особою, яка вже володіє майном, шляхом обману або зловживання довірою у таких формах: протиправне використання особою чужого майна, що перебуває в її віданні або розпорядженні, для одержання особистої вигоди (наприклад, самовільне використання транспортних засобів, механізмів, іншого майна); звернення на свою користь платежів, які повинні надійти від окремих громадян за послуги, особою не уповноваженою на їх одержання (наприклад, провідник вагону незаконно приймає пасажира та одержує від нього платіж за проїзд, обертаючи кошти на свою користь); неправомірне неповернення або несвоєчасне повернення майна або коштів, що позбавляє власника можливості їх використання на власний розсуд; ухилення від сплати обов'язкових платежів (наприклад, за житло, телекомунікаційні послуги, проїзд і т.п.); одержання майна або коштів з використанням пільг, на які винна особа не має прав [13, с. 210]. Якщо при цьому вчиняється злочин, передбачений статтею Розділу XVI КК, то потрібна додаткова кваліфікація за цією статтею.

Слід також звернути увагу на той факт, що значного поширення набули випадки заволодіння майном шляхом цілеспрямованого перекручення змісту комп'ютерної інформації, шляхом її зміни особою, яка має право доступу до неї (ст. 362 КК), або підробки шляхом несанкціонованого втручання (ст. 361 КК). Відповідно утворюється сукупність злочину проти власності та одного із указаних у цих статтях.

У якості прикладу можна навести такий випадок: студент одного з вузів міста вчинив несанкціоноване втручання в роботу комп'ютерної мережі місцевого провайдера Інтернет-послуг і перекрутив комп'ютерну інформацію про рахунки клієнтів та сплачений час роботи в мережі Інтернет (створив фіктивний рахунок). Після цього протягом кількох місяців безкоштовно користувався Інтернетом, чим заподіяв матеріальну шкоду провайдерові у розмірі 11000 грн. [14, с. 192].

Подібні випадки у світовій практиці дістали назву «крадіжка машинного часу». Такого роду злочинні посягання полягають у тому, що особа неправомірно використовує складне комп'ютерне устаткування (наприклад, суперкомп'ютери) або ресурси комп'ютерної мережі, абонентом або користувачем яких вона не є. Найбільш поширеним видом подібних

посягань у вітчизняній практиці є отримання доступу до мережі Інтернет за рахунок авторизованих абонентів шляхом використання їх акаунтів (логінів та паролів). Видається, що правильною кваліфікацією подібних дій є оцінка їх як сукупності злочинів, передбачених ст.ст. 192 та 361 КК. Однак, відповідальність за злочин, передбачений ст. 192 КК, настає лише у випадку заподіяння майнової шкоди, що перевищує 50 неоподатковуваних мінімумів доходів громадян. Оскільки шкода, що заподіюється внаслідок більшості фактів заволодіння чужим машинним часом, значно менша, подібні дії отримують правову оцінку як блокування комп'ютерної інформації законних користувачів у той час, коли за їх рахунок та під їх іменами порушники отримували доступ до інформації (ст. 361 КК), а також, якщо отримання чужих логінів і паролів здійснювалося шляхом несанкціонованого втручання або особою, яка має доступ до комп'ютерної інформації, відповідно до ст. 361 КК або ст. 362 КК.

Також на сьогодні одним з поширених кіберзлочинів є так званий «фішинг». Він полягає у тому, що зловмисники масово надсилають електронні листи, у яких від імені якогось відомого банку, Інтернет-магазину, фінансової компанії чи під іншим приводом, наприклад, виграш у лотереї, пропонують адресатам повідомити реквізити своєї платіжної картки або іншу важливу персональну інформацію, а потім використовують ці дані для заволодіння грошима адресатів або вчинення інших злочинів. Така злочинна діяльність у більшості випадків є транснаціональною, до якої, на жаль, все частіше залучаються й українські громадяни.

Наприклад, при розгляді клопотання про тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю, було встановлено, що невстановлені особи, що створили фішингові Інтернет-ресурси («card2card.su», «cardtocard.su», «oplaton.net», «oplator.net») під видом платіжних сервісів переказу грошових коштів CARD2CARD, за їх допомогою заволодівали платіжними реквізитами користувачів цих ресурсів. У подальшому ці особи здійснювали несанкціоновані перекази коштів з карток потерпілих на картки ПАТ «Укрсоцбанк» [15].

Знову ж таки дуже часто слідчі та суд розглядають такі випадки як шахрайство, вчинене з використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК). Проте така кваліфікація бачиться помилковою з таких підстав: у даному випадку викрадені дані не використовуються безпосередньо в ході обману чи зловживання довірою як спосіб заволодіння грошима. Обман чи зловживання довірою в даному випадку використовується як спосіб доступу до місця зберігання майна, а заволодіння ним вже відбувається в інший спосіб. У традиційній практиці правозастосування склалося відповідне правило кваліфікації таких випадків, закріплене у абз. 5 п. 17 Постанови: «Якщо обман або зловживання довірою були лише способом отримання доступу до майна, а саме вилучення майна відбувалося таємно чи відкрито, то склад шахрайства відсутній» [8]. У даному випадку спосіб таємний, отже і слід кваліфікувати такі діяння за ст. 185 КК.

Продовжуючи розгляд особливостей «комп'ютерних способів» вчинення злочинів проти власності, слід зауважити, що розповсюдженими є також випадки блокування роботи операційної системи програмою, яка повідомляє, що, якщо не буде переведено певну суму грошей на вказаний рахунок, вся інформація на носіях буде знищена, такі діяння повинні кваліфікуватися як вимагання (ч. 1 ст. 189 КК) та несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ч. 1 ст. 361 КК). Діяння в даному випадку полягає у вимозі передачі майна, а способом її підкріплення (забезпечення вимоги) є погроза знищення майна (інформації). Злочин у таких випадках вважається закінченим з моменту висунення вимоги передати гроші чи інше майно, незалежно від реалізації такої погрози.

Викрадення, пошкодження чи знищення комп'ютерної техніки – це звичайні злочини проти власності, тому труднощів із кваліфікацією таких дій не виникає. Але іноді пошко-

дження чи знищення комп'ютерної техніки може виступати як спосіб вчинення несанкціонованого втручання. Від останнього вони відрізняються насамперед за об'єктивними ознаками (об'єктом, предметом, об'єктивною стороною), але основною та визначальною ознакою розмежування вказаних злочинів проти власності від несанкціонованого втручання є спрямованість умислу. Якщо дії особи являють собою порушення фізичної цілісності комп'ютерної техніки, але мета, яку переслідує суб'єкт, полягає в заподіянні шкоди шляхом знищення інформації, то дії цієї особи слід кваліфікувати як несанкціоноване втручання в роботу ІТС, оскільки знищення або пошкодження комп'ютерної техніки в цьому випадку є способом вчинення вказаного злочину. Кваліфікувати подібні дії необхідно за правилами сукупності злочинів, передбачених ст. 361 і ст. 194 КК.

Цікавими є випадки вчинення злочинів проти власності за відсутності ознак злочинів, передбачених Розділом XVI КК. Цікавими вони є тому, що вчиняються з використанням прихованих та не використаних можливостей ІТС, які найчастіше не виявлені на етапах їх розробки та впровадження, але помічаються злочинцем і використовуються. Але ці можливості є легальними властивостями системи, вони не виникають під впливом зловмисника, а тому очевидне бажання кваліфікувати такі діяння за статтями Розділу XVI КК слід відкидати та кваліфікувати його відповідно до основного об'єкту посягання та інших ознак складу злочину. При вчиненні цих злочинів особа може використовувати недоліки технічних засобів чи програм або їхні особливості роботи.

Прикладом першого недоліку є можливість отримання з банкомату частини коштів з генерацією відміни операції без втручання в його роботу, яка донедавна існувала в банкоматах деяких банків. Полягала вона в тому, що при висуненні пачки купюр із пристрою видавання можливо було витягнути з неї частину купюр. Після певного часу, який відведено для витягнення коштів, банкомат фіксував їх залишення у пристрої та генерував відміну операції зняття коштів, отже сума на рахунку залишалася незмінною. Як видно, основа вчинення цього злочину лежить в особливостях технічного пристрою, який працює під управлінням програмного комплексу і ніякого втручання в його роботу чи змін в інформації не було вчинено. Такі дії слід кваліфікувати як банальну крадіжку (ст. 185 КК).

Прикладом другого типу використання можливостей ІТС при вчиненні злочину (врахування особливостей роботи програм) може слугувати спосіб заволодіння грошовими коштами, який віднедавна став дуже розповсюдженим. Касир невеличкого супермаркету помічає, що отримана виручка лише наприкінці місяця повністю звіряється з інформацією в комп'ютерній системі, а кожен день перед інкасацією та передачею до банку сума грошей просто підраховується і фіксується по факту. Використовуючи такі результати своїх спостережень, він (касир) частину коштів, які дають йому покупці, не кладе до каси, а присвоює і використовує їх на власний розсуд. Знову ж таки в даному випадку відсутній який-небудь незаконний вплив на комп'ютерну систему чи інформацію в ній, хоча її можливості використовуються. Кваліфікація повинна відбуватися лише за ч. 1 ст. 191 КК (привласнення чи розтрата чужого майна, яке було ввірене особі чи перебувало в її віданні).

Висновки. У ході кримінально-правової оцінки кіберзлочину проти власності слід чітко дотримуватися сталих положень правозастосування щодо необхідних ознак злочинів проти власності та злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Доцільно притримуватися таких основних правил:

1. За ч. 3 ст. 190 КК слід кваліфікувати діяння лише за наявності спрямованості обману чи зловживання довірою на людину, а під незаконними операціями з використанням електронно-обчислювальної техніки слід розуміти будь-які дії з використанням будь-якого її засобу, які суперечать положенням чинного законодавства. До таких, зокрема, відносять випадки заволодіння грошима покупців через розміщення на спеціалізованих сайтах неправдивих об'яв про продаж товарів або про надання послуг.

2. Усі інші діяння, у яких у механізмі незаконної передачі майна зловмиснику бере участь не людина, а технічний чи програмний засіб, слід вважати вчиненими таємним способом і кваліфікувати за ст. 185 КК. Сюди відносять випадки отримання шляхом обману

чи зловживання довірою інформації (облікових даних, реквізитів, паролів та логінів тощо), яка може бути використана для доступу до майна (так званий «фішинг»).

3. За наявності ознак обману чи зловживання довірою без ознак шахрайства слід застосовувати положення ст. 192 КК, враховуючи розмір шкоди, який вказаний у примітці до цієї статті. Сюди, зокрема, відносять випадки користування чужими акаунтами (обліковими записами) для доступу до мережі Інтернет, здійснення дзвінків тощо.

4. Не слід здійснювати посилання на статті Розділу XVI КК під час кваліфікації усіх злочинів проти власності, вчинених із використанням інформаційно-телекомунікаційних систем. Лише за наявності сукупності необхідних ознак складу злочину, що вказані в диспозиції (зокрема, предмет, суспільно небезпечні наслідки, спеціальний суб'єкт) або прямо витікають з неї (зокрема, форма вини), необхідна додаткова кваліфікація злочину проти власності разом із статтями Розділу XVI КК.

Список використаних джерел:

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

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 р. № 80/94-ВР / Верховна Рада України : Законодавство. – 05.11.2016 р. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

3. Дудоров О. О. Проблеми кваліфікації шахрайства / О. О. Дудоров // Політика в сфері боротьби зі злочинністю : матеріали міжнар. наук.-практ. Інтернет-конф. (11–16 берез. 2014 р.). – Івано-Франківськ, 2014. – С. 21–32 [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 Львівського державного університету внутрішніх справ. – 2014. – № 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. Шапочка С. В. Щодо поняття шахрайства, що вчиняється з використанням комп'ютерних мереж (кібершахрайства) / С. В. Шапочка // Вісник Асоціації кримінального права України. – 2015. – № 1(4). – С. 221–232.

7. Науково-практичний коментар Кримінального кодексу України / за заг. ред. Литвинова О. М. – Київ : Центр учбової літератури, 2016. – 536 с.

8. Про судову практику у справах про злочини проти власності : постанова Пленуму Верховного Суду України від 06.11.2009 № 10 [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/v0010700-09/print1478713805968879.

9. Кримінальне право України (у питаннях та відповідях) : навч. посіб. / кол. авторів Литвинов О. М., Житний О. О., Васильєв А. А. та ін.; за заг. ред. О. М. Литвинова. – Харків : ХНУВС, 2015. – 400 с.

10. Вирок Павлоградського міськрайонного суду Дніпропетровської області від 16 травня 2008 року в справі № 1-0604/2008 / Єдиний державний реєстр судових рішень [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/2065419.

11. Постанова Заводського районного суду м. Миколаєва від 23.04.2014 р. в справі № 487/2362/14-к / Єдиний державний реєстр судових рішень [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/38409638.

12. Ухвала Апеляційного суду Запорізької області від 04 червня 2015 року в справі № 335/8910/14-к / Єдиний державний реєстр судових рішень [Електронний ресурс]. –

Режим доступу: http://www.reyestr.court.gov.ua/Review/44743772.

13. Кримінальне право України. (Особлива частина) : підруч. / кол. авторів А. В. Байлов, О. А. Васильєв, О. О. Житний, та ін.; за заг. ред. О. М. Литвинова; наук. ред. серії О. М. Бандурка. – Харків : ХНУВС, 2011. – 572 с.

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

15. Ухвала Слідчого судді Малиновського районного суду м. Одеси від 27 вересня 2016 року в справі № 521/16482/16-к / Єдиний державний реєстр судових рішень [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/61619138.

Васильев Андрей Анатольевич,
кандидат юридических наук, доцент
(Харьковский национальный университет внутренних дел)

Пашнев Дмитрий Валентинович,
кандидат юридических наук, доцент
(Харьковский национальный университет внутренних дел)

ОСОБЕННОСТИ КВАЛИФИКАЦИИ КИБЕРПРЕСТУПЛЕНИЙ ПРОТИВ СОБСТВЕННОСТИ

В статье установлены особенности применения различных статей раздела VI Особой части Уголовного кодекса Украины при квалификации преступлений против собственности, совершаемых с использованием информационно-телекоммуникационных систем. Выявлены случаи дополнительной квалификации таких преступлений по статьям раздела XVI Особенной части Уголовного кодекса Украины.

Ключевые слова: *киберпреступление, информационно-телекоммуникационная система, преступления против собственности, уголовно-правовая оценка, квалификация.*

Vasyliev A.A.,
candidate of law sciences, associate professor
(Kharkiv National University of Internal Affairs)

Pashniev D.V.,
candidate of law sciences, associate professor
(Kharkiv National University of Internal Affairs)

FEATURES OF QUALIFICATION OF CYBERCRIMES AGAINST PROPERTY

This article establishesfeatures of usingof various articles of Title VI of the Special Part of the Criminal Code of Ukrainein the qualificationof crimes against property committed through the use of information and telecommunication systems. Illustratedcases of additional qualifications of this crimes under articles of Title XVI of the Special Partof the Criminal Code of Ukraine.

Keywords: *cyber-crime, crime against property, criminal law qualification*

Надійшла до редколегії 15.09.2016