УДК 343.537:343.346.8:343.974

ПРОБЛЕМИ КВАЛІФІКАЦІЇ ШАХРАЙСТВА З ВИКОРИСТАННЯМ ЕЛЕКТРОННО-ОБЧИСЛЮВАНИХ МАШИН

PROBLEMS OF QUALIFICATION OF SHEEP WITH USING ELECTRONIC COMPONENT MACHINES

Драгоненко А.О.,
кандидат юридичних наук, доцент,
доцент кафедри галузевого права та правоохоронної діяльності
Центральноукраїнського державного
педагогічного університету імені Володимира Винниченка

Ніколенко М.І.,
студентка
факультету історії та права
Центральноукраїнського державного
педагогічного університету імені Володимира Винниченка

Статтю присвячено проблемі кваліфікації шахрайства з використанням електронно-обчислюваних машин. Розглянуто питання відмежування шахрайства в його доктринальному тлумаченні від викрадення з використанням комп'ютерних технологій – кібершахрайства.
Ключові слова: зловживання довірою, комп'ютерне шахрайство, шахрайство.

Статья посвящена проблеме квалификации мошенничества с использованием компьютерных технологий. Рассмотрены вопросы отделения мошенничества в его доктринальном толковании от хищений с использованием компьютерных технологий – кибермошенничества.
Ключевые слова: злоупотребление доверием, компьютерное мошенничество, мошенничество.

The article is devoted to the problem of qualification of fraud using computer technologies. The issues of delimitation of the concepts of fraud in its doctrinal interpretation from the theft using computer technologies – cyber crime reconsidered.
Key words: abuse of trust, computer fraud, fraud.

Постановка проблеми. На даний час, у століття розвитку інформаційних технологій, усі сфери життя суспільства поступово починають переходити на вищий щабель розвитку, все частіше використовується технічне забезпечення у вигляді комп'ютерів і мережі Інтернет. Якщо звернути увагу на стан інформаційних технологій десять років тому і зараз, то можна зробити висновок, що комп'ютерна інформація не стоїть на місці і впроваджується в усі сфери життя суспільства. Наприклад, використання кредитних карт як засобу зберігання грошових коштів, оплата комунальних послуг за допомогою мережі Інтернет, передача важливої інформації через соціальні мережі, використання електронного цифрового підпису. Тобто можна привести безліч прикладів зі сфери суспільних відносин, де широко використовується комп'ютерна інформація. Інформаційні технології багато в чому полегшили життя і діяльність суспільства, але водночас спричинили нові проблеми як у моральній, так і в матеріальній сфері життя людини, саме людини, тому що зазвичай роль користувача комп'ютерних технологій завжди відіграє людина, незалежно від її статусу та цілей використання цих технологій. У зв'язку із цим підвищився і рівень злочинності у сфері комп'ютерної інформації.

Глобалізація світової економіки впливає також на вигляд роздрібної торгівлі, більшість товарів і послуг, які люди могли отримати з рук у руки, зараз можна віднайти в мережі Інтернет. Виник новий вид злочинів, як-от шахрайство з використанням електронно-обчислювальних машин (далі – ЕОМ), який кваліфікується за ч. 3 ст. 190 Кримінального кодексу України (далі – КК України).

Зараз є проблема неоднозначної кваліфікації цього виду шахрайства, оскільки правоохоронні органи не завжди визнають мережу Інтернет, оголошення і торгові ресурси за необхідний інструмент та кваліфікуючу ознаку в цьому виді злочину. Тобто вищезазначені дії кваліфікуються як звичайне шахрайство (ч. 1. ст. 190 КК України) або шахрайство, вчинене повторно (ч. 2 ст. 190 КК України), використання ж ЕОМ і комп'ютерних мереж не береться до уваги, що прямо впливає на кваліфікацію даного злочину. На наш погляд, незважання на використання ЕОМ і комп'ютерних мереж призводить до неправильної кримінально-правової кваліфікації злочинів.

Наприклад, так званий фішинг – технологія, яка полягає в крадіжці конфіденційних даних, також набуло поширення шахрайство у сфері комп'ютерної інформації. Тому виникла потреба ввести санкції проти осіб, які вчиняють злочини в цій сфері. Але тоді постало питання, як кваліфікувати такий вид злочинів? Зараз це питання актуальне не тільки для національної кримінально-правової доктрини, а й на міжнародному рівні загалом, що підтверджує значущість даної проблеми.

Стан опрацювання. Проблематику кваліфікації злочинів проти власності з використанням ЕОМ розглядали такі відомі вчені, як: Д.С. Азаров, А.А. Музика, М.І. Панов, В.О. Навроцький, Н.А. Савінова, А.В. Савченко та інші. Проте деякі з юридичних моментів потребують аналізу.

Метою статті є розгляд неоднозначного підходу до кваліфікації шахрайств, вчинюваних за допомогою використання ЕОМ і комп'ютерних мереж.

Виклад основного матеріалу. Поняття «комп'ютерне шахрайство» з'явилося ще в 70-і рр. минулого століття, коли в розвинених країнах підвищився рівень економічних злочинів [1], тому з'явилася потреба реформувати законодавство, але законодавці були дещо спантеличені, бо, з одного боку, здавалося б, що можна просто додати кваліфікуючі ознаки до чинних норм, але, якщо детально розібрати конструкцію цього виду злочину, то можна помітити, що з'явився як новий спосіб, так і новий предмет посягання, тому виникла необхідність ввести нові склади в кримінальні кодекси, що передбачають відповідальність за такі злочини.

Щоб скласти загальне враження про злочини у сфері комп'ютерної інформації та провести аналіз кваліфікації цих злочинів у різних країнах, необхідно навести при-

клад кібершахрайства. Одним із поширених прикладів кібершахрайства, яке властиве багатьом країнам, є фішинг [2], сутність якого можна пояснити так: шахрай, обманюючи користувача, змушує його надати свою конфіденційну інформацію: дані для виходу в Інтернет (ім'я та пароль), інформацію про кредитні картки тощо. Варто зазначити, що всі дії жертва виконує абсолютно добровільно, не розуміючи, що вона робить насправді. Для цього використовуються технології соціальної інженерії. Сьогодні є три різновиди фішингу – поштовий, онлайновий і комбінований. Поштовий – найстаріший. На електронну пошту надсилається спеціальний лист із вимогою вислати будь-які дані. Онлайн-фішингом передбачає, що зловмисники копіюють будь-які сайти (найчастіше це інтернет-магазини). Водночас використовуються схожі доменні імена й аналогічний дизайн. Ну а далі все просто. Жертва, потрапляючи в такий магазин, вирішує придбати товар. Кількість таких жертв досить велике, адже ціни в такому «магазині» будуть дуже низькими, а всі підозри розсіюються через популярність сайту. Купуючи товар, жертва реєструється і вводить номер та інші дані своєї кредитної картки. Такі способи фішингу наявні вже досить давно. Завдяки поширенню знань у сфері інформаційної безпеки вони поступово перетворюються на неефективні способи відбирання грошей.

В Україні сьогодні точаться дискусії щодо протидії кіберзлочинам і здійснення кримінального судочинства. Організація Об'єднаних Націй (далі – ООН) визнає нагальність зазначеної проблеми. Адже постійний розвиток технологій зумовлює також зміни способів вчинення кіберзлочинів. В Україні поки немає термінологічного поняття кіберзлочинності, але вже із травня 2018 р. набуває чинності Закон України «Про основні засади забезпечення кібербезпеки України», який містить усі поняття щодо злочинів, пов'язаних із комп'ютерною діяльності.

Відповідно до ч. 3 ст. 190 КК України, злочином вважається шахрайство, вчинене шляхом незаконних операцій із використанням ЕОМ, законодавство також не надає визначення цього поняття. Незважаючи на це, р. XVI КК України називається «Злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», визначає відповідальність за вчинення злочинів із використанням ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж. Але і в ньому не визначається, які пристрої входять до ЕОМ.

Шахрайство розуміють як заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою. Особа, щодо якої скоюється злочин, добровільно передає майно або право на це майно, що не завжди характерно для злочинів, вчинених у сфері комп'ютерної інформації. Найчастіше і разі комп'ютерного шахрайства потерпілий дізнається про несприятливі наслідки скоєного тільки через певний проміжок часу, наприклад, перевіривши баланс своєї кредитної картки і побачивши нульовий результат. Отже, відсутня одна з важливих ознак складу злочину – добровільність. Також необхідно звернути увагу на два терміни, що вживаються у визначенні поняття шахрайства: «обман» і «зловживання довірою» Одразу ж постає запитання: що або хто в цьому разі є об'єктом обману? За логікою законодавця, особа, яка скоїла злочин, обманює комп'ютер і заволодіває майном іншої особи. З іншого боку, йдеться про обман або зловживання довірою як про об'єктивну сторону складу шахрайства; водночас у ролі об'єкта обману завжди виступає фізична особа, отже, у складі злочину шахрайства потерпілою особою завжди є фізична особа, а ніяк не комп'ютер або комп'ютерна інформація. Під час шахрайства необхідний безпосередній або опосередкований контакт між особою, яка вчиняє злочин, тобто злочинцем, і між потерпілим, бо впливу зазнає насамперед психіка людини, а маніпуляція комп'ютерними даними має суто технічний характер.

Якщо звернутися до міжнародної практики, то в Німеччині, наприклад, такі дії кваліфікуються, як «намір отримати для себе або третьої особи майнову вигоду, шляхом завдання шкоди майну іншої особи, впливаючи на результат обробки даних внаслідок неправильного створення програм, використання неправильних або неповних даних, шляхом неправомірного використання даних або іншого неправомірного впливу на результат обробки даних» (ст. 263а) [3], а в Кримінальному кодексі Австрії – як «майнова шкода, завдана з метою отримання незаконної вигоди для злочинця або третьої особи, шляхом впливу на процеси автоматизованої обробки даних за допомогою спеціальних програм, введення, зміни або знищення даних або іншим способом, що впливає на процес обробки даних» (ст. 148а) [3]. З формулювання цих статей можна зрозуміти, що об'єктом є не комп'ютер або процеси автоматизованої обробки даних, а спеціальні програми як спосіб, за допомогою якого особа вчиняє діяння. Можливо, таке формулювання є найбільш правильним. Під час аналізу складу шахрайства виявляються істотні суперечності стосовно злочинів у сфері комп'ютерної інформації, ці протиріччя проявляються як в об'єкті, так і в кваліфікуючих ознаках. Зараз це питання актуальне для кримінального законодавства України. На законодавчому рівні пропозицій щодо вирішення цієї проблеми поки не вносилося, однак деякі вчені висловили свою думку щодо цього. Так, В.Б. Вєхов, Ю.І. Ляпунов, В.Ю. Максимов, М.А. Селіванов допускають наявність терміна «комп'ютерний злочин» у кримінологічному і криміналістичному аспектах. М.А. Селіванов вважає, що необхідно більш широко тлумачити цей термін, включаючи в його розуміння всі злочини, вчинені з використанням комп'ютерної техніки [4, с. 46]. Т.Л. Тропіна визначає кіберзлочинність як сукупність злочинів, учинених у кіберпросторі за допомогою або з використанням комп'ютерних систем чи комп'ютерних мереж, а також інших засобів доступу до кіберпростору, у рамках комп'ютерних систем або мереж і проти комп'ютерних систем, комп'ютерних мереж й комп'ютерних даних [5, с. 19]. Це визначення відповідає рекомендаціям експертів ООН. На їхню думку, термін «кіберзлочинність» охоплює будь-який злочин, що вчиняється з використанням комп'ютерної системи або мережі, у рамках комп'ютерної системи або мережі, проти комп'ютерної системи або мережі. Отже, до кіберзлочинів може бути віднесено будь-який злочин, учинений в електронному середовищі – кіберпросторі. Авторське визначення кібершахрайству надав С.В. Шапочка: «Кібершахрайство – кіберзлочин, що полягає в заволодінні чужим майном або надбанні права на майно шляхом обману чи зловживання довірою та вчиняється в кіберпросторі за допомогою або з використанням комп'ютерно-телекомунікаційних пристроїв, систем чи мереж, а також інших засобів доступу до кіберпростору в рамках комп'ютерних систем або мереж і проти комп'ютерних систем, комп'ютерних мереж й комп'ютерних даних» [6, с. 231].

Поруч із розбіжністю науковців наявні розбіжності і в практичному застосуванні досліджуваного поняття.

У Єдиному державному реєстрі судових рішень за пошуковим запитом за категоріями «вирок», «кримінальне судочинство», "aukro" було отримано відомості щодо 46 вироків. Ці судові рішення пов'язані з кримінально-правовою оцінкою посягань на чуже майно шляхом обману – розміщення на сайті інтернет-аукціону "Aukro" неправдивих повідомлень щодо продажу окремих товарів.

З огляду на те, що сьогодні "Aukro" є найбільш популярним національним інтернет-аукціоном, отриману сукупність судових рішень можна обґрунтовано вважати репрезентативною добіркою. Головний результат аналізу названої сукупності вироків такий: сьогодні в судовій практиці є два підходи до кримінально-правової кваліфікації шахрайства, вчиненого з використанням інтернет-аукціонів [7].

Так, у 36 випадках (78%) дії винних осіб розглядалися як шахрайство, вчинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК України).

Водночас у 10 випадках (22%) такі ж діяння розглядалися як злочини, передбачені ч. 1 ст. 190 або ч. 2 ст. 190 КК України, кваліфікуюча ознака «шляхом незаконних операцій з використанням електронно-обчислювальної техніки» не інкримінувалася. Деякі із судових рішень останньої категорії містять обґрунтування здійсненої кваліфікації.

Так, у вироку Кіровського районного суду м. Кіровограда від 12 вересня 2013 р. в справі № 404/5170/13-к зазначається: «Згідно з диспозицією ч. 3 ст. 190 КК України, кваліфікуючими ознаками кримінального правопорушення є шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій із використанням електронно-обчислювальної техніки, при цьому поняття електронно-обчислювальної техніки та незаконних операцій, які можуть спричинити майнову шкоду, визначені в ст. ст. 361–363 КК України» [1].

Як вбачається зі змісту повідомлення про підозру й обвинувального акта, у даному конкретному разі особу звинувачено в заволодінні чужим майном шляхом обману та зловживання довірою, а також шляхом незаконних операцій із використанням електронно-обчислюваної техніки, яке виразилося в розміщенні на сайті інтернет-аукціону «Емаркет Україна» завідомо неправдивої інформації.

У вироку Луцького міськрайонного суду Волинської області від 31 липня 2012 р. в справі № 0308/8267/12 зазначено: «Органом досудового слідства дії підсудного кваліфіковані за ч. 3 ст. 190 КК України за кваліфікуючою ознакою – вчинення шахрайства шляхом незаконних операцій із використанням електронно-обчислювальної техніки. На думку суду, вказане не знайшло свого підтвердження.

Електронно-обчислювальна техніка – це комплекс технічних засобів, призначених для автоматичної обробки інформації в процесі вирішення обчислювальних та інформаційних завдань. Операція з використанням електронно-обчислювальної техніки має бути незаконною, тобто такою, що не відповідає вимогам законодавства. Зважаючи, що підсудним таких дій вчинено не було, оскільки перерахування коштів на рахунок через банківську установу або банківським переказом не є незаконною операцією, тому дії підсудного із вказаних епізодів підлягають перекваліфікації із ч. 3 на ч. 2 ст. 190 КК України, за кваліфікуючою ознакою – вчинення дій повторно» [8].

У вироку Олександрійського міськрайонного суду Кіровоградської області від 5 березня 2013 р. у справі № 398/10/13-к 1-кп/398/23/13 зазначено: «Аналізуючи зібрані докази та оцінюючи їх разом, суд вважає, що в судовому засіданні повністю підтвердився факт вчинення обвинуваченим повторного заволодіння чужим майном шляхом обману та зловживання довірою, а тому він повинен нести відповідальність за ч. 2 ст. 190 КК України. Суд виключає з обвинувачення таку ознаку, як заволодіння чужим майном шляхом незаконних операцій із використанням електронно-обчислювальної техніки, оскільки комп'ютерна мережа не є електронно-обчислювальною технікою, а лише електронною. Крім того, такі операції законом не передбачені» [9].

Аргументи, що наводяться у вказаних судових рішеннях, викликають зауваження. Так, очевидно, що тлумачення терміна «незаконна операція з використанням електронно-обчислювальної техніки» як вчинення підсудним одного зі злочинів, передбачених ст. ст. 361–363–1 КК України, є невиправдано обмежувальним. Не викликає сумнівів те, що використання комп'ютерної техніки для здійснення банківських розрахунків не є незаконною операцією, але як така розглядається розміщення на спеціалізованому інтернет-ресурсі завідомо неправдивого повідомлення. Нарешті, вказівка на те, що комп'ютерна мережа «не є електронно-обчислювальною технікою, а лише електронною», суперечить загальновизнаним положенням інформатики. Здається, що інкримінування кваліфікуючої ознаки, передбаченої ч. 3 ст. 190 КК України, у разі вчинення шахрайства з використанням спеціалізованих інтернет-ресурсів, призначених для розміщення повідомлень щодо продажу товарів, обґрунтовано. Комп'ютерна мережа (зокрема Інтернет), за визначенням, становить сукупність територіально розосереджених систем опрацювання даних, засобів і (або) систем зв'язку та передавання даних, що забезпечує користувачам дистанційний доступ до її ресурсів і колективне використання цих ресурсів.

Отже, розміщення повідомлення на спеціалізованому сайті є використанням інформаційного ресурсу шляхом дистанційного доступу до нього, забезпеченим засобами електронно-обчислювальної техніки, тобто є операцією з використанням ЕОМ. По-друге, розміщення завідомо неправдивого повідомлення щодо продажу товарів або надання певних послуг, із позицій Закону України «Про захист прав споживачів», є нечесною підприємницькою практикою, яка, відповідно до ст. 19 Закону, заборонена.

Крім того, вчинення означених дій порушує також загальні норми Цивільного кодексу (далі – ЦК) України. Зокрема у ст. 13 ЦК України зазначається, що під час здійснення своїх прав особа зобов'язана утримуватися від дій, які могли б порушити права інших осіб, не допускаються дії особи, що вчиняються з наміром завдати шкоди іншій особі, а також зловживання правом в інших формах. Отже, розміщення завідомо неправдивого повідомлення щодо продажу товарів або надання певних послуг треба розглядати як незаконне.

Порушена в роботі проблема не може вважатися розв'язаною без розгляду ще одного аспекту. Наскільки обґрунтовано положення чинного законодавства щодо розгляду шахрайства, вчинюваного шляхом незаконних операцій із використанням електронно-обчислювальної техніки, як тяжкого злочину? Застосування комп'ютерної техніки для здійснення шахрайства справді може свідчити про підвищену суспільну небезпечність посягання. Поширеність засобів електронної комерції, систем дистанційного банківського обслуговування раніше була незначною. Користувалися ними великі господарюючі суб'єкти. Тому положення ч. 3 ст. 190 КК України доволі чітко окреслювали коло діянь, які обґрунтовано розглядалися як особливо кваліфікований вид шахрайства, близький за ступенем суспільної небезпечності до шахрайства у великих розмірах. Проте стрімкі темпи проникнення інформаційних технологій у фінансову сферу зумовили якісну зміну цього виду шахрайства.

Правоохоронні органи фіксують відчутну кількість таких злочинів, зв'язаних із завданням шкоди, що відповідає ознакам простого або кваліфікованого шахрайства (ч. ч. 1, 2 ст. 190 КК України). Чи можна вважати обґрунтованою, а саме цього вимагає тлумачення норми, кримінально-правову оцінку таких дій за ч. 3 ст. 190 КК України? У сучасних умовах немає підстав стверджувати, що використання електронно-обчислювальної техніки в процесі здійснення шахрайства настільки підвищує рівень суспільної небезпечності вчиненого діяння. З огляду на зазначене, доцільною здається відмова від нормативного закріплення такої кваліфікуючої ознаки.

В умовах стрімкого розширення сфери застосування інформаційних технологій положення ч. 3 ст. 190 КК України набувають характеру таких, які не забезпечують адекватне кримінально-правове відображення об'єктивного рівня розвитку суспільних відносин. Формалізовані в цій нормі уявлення законодавця про суспільну небезпечність шахрайства, вчинюваного шляхом незаконних операцій із використанням електронно-обчислювальної машин, не відповідають фактичному рівню розвитку відносин інформатизації. Унаслідок цього законодавча оцінка суспільної

небезпечності посягань (покарання до 8 років позбавлення волі) не відповідає рівню їхньої фактичної суспільної небезпечності.

Нарешті, розгляд ситуації, що виникла, був б неповним без аналізу ще одного аспекту проблем. З огляду на зміст ст. 246 КПК України, більшість негласних слідчих (розшукових) дій проводяться виключно в кримінальних провадженнях у тяжких або особливо тяжких злочинах (злочин, передбачений чинною редакцією ч. 3 ст. 190 КК України, є тяжким).

Специфіка шахрайства, що здійснюється з використанням електронно-обчислювальної техніки, зумовлює необхідний характер таких дій. Зокрема, результативне розслідування цієї категорії злочинів практично нездійсненно без зняття інформації з електронних інформаційних систем. Маємо абсурдну ситуацію: наявність у КК України норми, яка не відповідає соціальним тенденціям і не відображає об'єктивну небезпечність передбаченого діяння, дозволяє «спрацьовувати» нормам КПК, правоохоронні органи мають підстави для проведення необхідних негласних слідчих (розшукових) дій.

Очевидно, що наведені положення не варто розглядати як аргумент на користь збереження ч. 3 ст. 190 КК України в чинній редакції. Ситуацію, що виникла, варто розглядати як ще одне підтвердження необґрунтованості законодавчого обмеження сфери застосування негласних слідчих (розшукових) дій, недоцільності залежності можливості їх проведення від тяжкості вчиненого злочину. У цьому контексті заслуговують на позитивну оцінку та підтримку пропозиції Управління боротьби з кіберзлочинністю Міністерства внутрішніх справ України щодо доповнення ст. 246 КПК України положеннями про можливість проведення негласних слідчих (розшукових) дій у кримінальних провадженнях щодо злочинів, учинених із використанням електронно-обчислювальної техніки, незалежно від ступеня їх тяжкості. Збереження наявного порядку застосування негласних (слідчих) розшукових дій у кримінальних провадженнях щодо злочинів такої категорії практично унеможливлює ефективну діяльність правоохоронних органів у цій сфері.

Висновки. Отже, до проблем кібербезпеки в Україні не серйозно ставляться правоохоронні органи. Неправильна також кваліфікація зазначеного виду шахрайства, тому що не завжди правоохоронці звертають увагу на мережу Інтернет, онлайн-магазини й інші торгові ресурси як кваліфікуючу ознаку в цьому злочині. Адже вищезгадані дії кваліфікуються зазвичай як звичайне шахрайство (ч. 1. ст. 190 КК України) або як шахрайство, вчинене повторно (ч. 2 ст. 190 КК України), але водночас використання ЕОМ і комп'ютерних мереж, що прямо впливає на кваліфікацію такого правопорушення, не враховується. Незважання на використання ЕОМ і комп'ютерних мереж призводить до неправильної кримінально-правової кваліфікації злочинів, це засвідчується результатами досліджень судової практики, які пов'язані із засудженням за шахрайські дії з використанням інтернет-аукціонів, що містять відомості про призначення реальних покарань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Susan H. Nycum. The Criminal Law Aspects of Computer Abuse: Applicability of the State Penal Laws to Computer Abuse (Menlo Park, California, Stanford Research Institute, 1976). Ulrich Sieber, Computerkriminalität und Strafrecht (Cologne, Karl Heymanns Verlag, 1977). URL: http://www.worldcat.org/title/criminal-law-aspects-of-computer-abuse-applicability-of-the-state-penal-laws-to-computerabuse/oclc/654145221/editions?referer=di&editionsView=true.
2. Вікіпедія. URL: https://uk.wikipedia.org/wiki/%D0%A4%D1%96%D1%88%D0%B8%D0%BD%D0%B3.
3. Карпович О.Г. Анализ актуальных проблем противодействия законной предпринимательской деятельности в уголовном законодательстве некоторых европейских государств. URL: http://www.lawmix.ru/comm/771.
4. Номоконов В.А., Тропинина Т.Л. Киберпреступность как новая криминальная угроза. Криминология: вчера, сегодня, завтра: журн. Санкт-Петербург. междунар. криминолог. клуба. 2012. № 1 (24). С. 45–55.
5. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дисс. ... канд. юрид. наук: 12.00.08. Владивосток, 2005. 235 с.
6. Шапочка С.В. Щодо поняття шахрайства, що вчиняється з використанням комп'ютерних мереж (кібершахрайства). Вісник Асоціації кримінального права України. 2015. № 1 (4) С. 221–232.
7. Карчевський М.В. Особливості кваліфікації шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки. Науковий вісник Львівського державного університету внутрішніх справ. Серія «Юридична». Вип. 1. 2014. С. 272–281.
8. Вирок Луцького міськрайонного суду Волинської області від 31 липня 2012 р. у справі № 0308/8267/12 / Єдиний державний реєстр судових рішень. URL: ttp://reyestr.court.gov. ua/Review/25437127.
9. Вирок Олександрійського міськрайонного суду Кіровоградської області від 5 березня 2013 р. у справі № 398/10/13- к 1-кп/398/23/13 / Єдиний державний реєстр судових рішень. URL: http://reyestr.court.gov.ua/Review/29790333.