УДК 343.431:343.985

В.Г. Телійчук
кандидат юридичних наук, доцент
Кіровоградський інститут державного та муніципального управління Класичного приватного університету

СПОСОБИ ВЧИНЕННЯ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ ТА ЗАХОДИ ПРОТИДІЇ

У статті розглянуто способи вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, визначено розподіл злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку за типами. Досліджено вчинення зазначених злочинів організованою злочинністю, яка відзначається високою ймовірністю соціальної небезпеки, складністю виявлення, встановлення вини й збирання доказів. Визначено особливості вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку організованими злочинними групами. Звернуто увагу на вчинення зазначених злочинів у банківській сфері, розкрито основні способи вчинення. Здійснено дослідження статистичних показників вчинення зазначених злочинів за останні два роки, що характеризуються появою в Україні нового типу шахрайства з банкоматами. Розглянуто заходи протидії злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Ключові слова: *транснаціональні злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, криміналістика, оперативно-розшукова діяльність, злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, що вчиняються організованою злочинністю, способи вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, що вчиняються організованою злочинністю, особливості вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, що вчиняються організованою злочинністю, системи розмежування доступу, співпраця у сфері боротьби з "картковою" злочинністю.*

І. Вступ

Актуальність теми дослідження зумовлена стрімким розвитком нового виду протиправної діяльності – транснаціональних злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; різким підвищенням кримінального комп'ютерного професіоналізму; активною міграцією злочинців і організованістю їх дій, що суттєво ускладнює криміногенну обстановку і є складним феноменом, який вимагає інтеграції багатьох галузей знань, зокрема, юридичної науки для поглибленого дослідження природи цих злочинів, особливостей їх криміналістичної характеристики, тактики виявлення та запобігання з урахуванням сучасних досягнень вітчизняної й зарубіжної теорії та практики криміналістики [1] й оперативно-розшукової діяльності [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 визначає: "…Комп'ютерна злочинність – це особливий вид злочинів, пов'язаних із незаконним використанням сучасних інформаційних технологій і засобів комп'ютерної техніки. В їх основі можуть бути політичні, хуліганські, корисливі й інші мотиви. Це зумовлює необхідність розвитку й удосконалення правових засобів регулювання суспільних відносин у сфері інформаційної діяльності…" [3].

Різним аспектам злочинів у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, способам і механізму їх вчинення, технології та техніці виявлення й закріплення слідів, тактиці проведення слідчих та оперативно-розшукових дій приділялено увагу в наукових працях вітчизняних і зарубіжних учених: В.Г. Афанасьєва, Ю.М. Батуріна, В.П. Бахіна, Л.В. Борисової, А.Б. Венгерова, В.Б. Вєхова, Н. Вінера, В.П. Гавловського, О.А. Гаврилова, В.О. Голубєва, М.В. Гуцалюка, І.З. Карася, В.В. Кри-

лова, В.Д. Курушина, В.П. Меживого, В.О. Мещерякова, Д.И. Никифорчука, М.С. Полєвого, В.Ю. Рогозіна, С.Г. Рогозіна, К.В. Тітуніної, І.Ф. Хараберюша, М.Г. Шурухнова та ін.

II. Постановка завдання

Мета статті – на основі сучасних вітчизняних і зарубіжних концепцій науки криміналістики та оперативно-розшукової діяльності розробити тактичні й процесуальні основи дослідження злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (далі – комп'ютерні злочини), рекомендації щодо їхнього виявлення, запобігання, протидії, розкриття та розслідування.

III. Результати

Важливим сучасним завданням правової науки, нормотворчості та правоохоронної діяльності є створення гарантій збалансованого співвідношення інтересів особи й держави в боротьбі зі злочинністю.

Соціально-економічний і науково-технічний розвиток України на сучасному етапі пов'язані з вирішенням проблем інформатизації держави, суспільства, правопорядку. Інформаційне забезпечення оперативно-розшукової діяльності є складовою інформатизації правоохоронних органів, що є невід'ємною частиною інформаційної системи України [2, с. 184].

У сучасному світі інформація є найцінніше глобальним ресурсом. Економічний потенціал суспільства переважно визначається обсягом інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Інформація постійно ускладнюється, змінюється якісно, зростає кількість її джерел і споживачів. Водночас зростає вразливість сучасного інформаційного суспільства від недостовірної (а іноді й шкідливої) інформації, її несвоєчасного надходження, промислового шпигунства, злочинів у сфері використання комп'ютерних мереж тощо. Тому Конституція України забезпечення інформаційної безпеки відносить до найважливіших функцій держави [4, с. 281].

Більшість фахівців поділяють комп'ютерні злочини на два типи:

1. Злочини, в яких об'єктом їх здійснення є комп'ютери: знешкодження або заміна даних, програмного забезпечення та обладнання; розкрадання вхідних, вихідних даних, програмного забезпечення та обладнання; економічне шпигунство та розголошення відомостей, які становлять державну чи комерційну таємницю; інші злочинні діяння цього виду.

2. Протизаконні дії, для здійснення яких комп'ютери використовуються як знаряддя в досягненні злочинної мети: комп'ютерний саботаж; вимагання та шантаж; розтрата; розкрадання коштів; обман споживачів, інвесторів чи користувачів; інші злочини.

До категорії "інші злочинні діяння" віднесено несанкціоноване використання комп'ютера в особистих цілях [5, с. 111].

Масова комп'ютеризація, яка розпочалася в кінці 80-х – на початку 90-х рр. XX ст., привела до розвитку ринку комп'ютерів і програмного забезпечення, значно розширила сферу застосування електронно-обчислювальних машин (ЕОМ), які все частіше підключаються до мережі широкого доступу.

Активно упроваджується автоматизована обробка бухгалтерської й іншої документації, "безпаперові" технології. Інформація, що міститься в комп'ютері, найчастіше не зберігається на папері. Комп'ютер став практично обов'язковим елементом робочого столу не тільки керівника підприємства, а й працівників.

Наслідком цих процесів є криміналізація сфери використання комп'ютерних технологій. Більшість таких злочинів вчиняється в кредитно-фінансовій сфері, проте комп'ютерну інформацію використовують і в "традиційних" злочинах, таких як шахрайство, фальшивомонетництво, наприклад: для фальсифікації платіжних документів; розкрадання готівки й безготівкових грошей шляхом переведення на фіктивні рахунки; "відмивання" грошей; повторного отримання виплат; купівлі з використанням фальсифікованих або вкрадених кредитних карток; продаж таємної (конфіденційної) інформації.

Поняття "комп'ютерна злочинність" та його трансформування в поняття злочинів у сфері інформаційних технологій ми досліджували раніше, тому немає сенсу зупинятися на цих питаннях [6]. Лише слід нагадати, що виявлення й розкриття комп'ютерних злочинів, особливо таких, що вчиняються організованими злочинними угрупованнями, вимагає спеціальної фахової освіти та високого інтелектуального рівня працівників правоохоронних органів, їм потрібно мати добрі знання не тільки в галузі права, а й у галузі інформатики.

Дослідження свідчать, що злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, що вчиняються організованою злочинністю, відзначається високою ймовірністю соціальної небезпеки, складністю виявлення, встановлення вини й збирання доказів. Особливістю злочинів у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є й те, що вони можуть вчинятися з використанням засобів комунікацій віддаленого доступу, що не потребує присутності правопорушника на безпосередньому місці вчинення злочину (у традиційному розумінні). Останнім часом спо-

стерігається тенденція до зрощення комп'ютерної злочинності з традиційною організованою злочинністю, інтернаціоналізації цього виду злочинів. Це виявляється в несанкціонованому проникненні в банківські кредитно-розрахункові комп'ютерні системи, електронну торгівлю, зокрема через Інтернет, у тому числі шахрайстві з магнітними картками тощо.

Особливістю злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, що вчиняються групою осіб, є обов'язкова наявність такого специфічного учасника злочинної групи, як хакер (фрікер, крекер тощо). Цим жаргонним терміном називають особу, яка володіє знаннями й навичками несанкціонованого проникнення до комп'ютерної системи. Вона є основним виконавцем цього злочинного діяння [6, с. 199].

Сьогодні злочинним шляхом використовують електронно-обчислювальну техніку, насамперед у банківській системі. Хоча в умовах ринкових відносин предметом розкрадання може бути й інформація різного значення. Не є таємницею, що організовані злочинні угруповання мають у своїх "штатах" спеціалістів, які займаються розвідкою з використанням найсучасніших технічних засобів для збирання необхідної інформації про діяльність конкурентів, засобів масової інформації, підприємств та фірм, які перебувають у межах їх інтересів, і правоохоронних органів. Термін "комп'ютерні злочини" був розроблений для визначення як абсолютно нового виду злочинності, що орієнтуються на комп'ютери, телекомунікаційні мережі та їх користувачів, так і для більш традиційних злочинів, для здійснення яких сьогодні використовують комп'ютерне обладнання. Серед комп'ютерних злочинів, вчинених у світі, все більше стає "міжнародних", таких, які як засоби або жертви використовують інформаційні системи різних держав світу, з можливістю доступу до національних, у тому числі й спеціально захищених інформаційних ресурсів, що створює нові умови для організованої злочинності – використання Інтернет не тільки для здійснення правопорушень, а й для організації віртуальних банд.

Банківська система життєдіяльності держави, яка пов'язана з накопиченням, розподілом і використанням державних та приватних коштів, є однією з найбільш привабливих для окремих злочинців і особливо організованих злочинних груп. У цій системі на теперішній час вчиняється значна кількість різних фінансових афер, здійснюваних частіше за все при різних банківських операціях. Злочини, що вчиняються в банківській системі або з її використанням, можна віднести до одних із найбільш небезпечних економічних злочинів, оскільки їх негативний вплив позначається не тільки на самому банку, а й на багатьох інших суб'єктах економічної діяльності та фінансовій системі держави загалом. Способи вчинення банківських злочинів дуже різноманітні. Найбільш поширені з них ті, що вчиняються з використанням сучасних інформаційних технологій: підробка та використання пластикових платіжних карток та комп'ютерної банківської інформації. За даними Управління боротьби з кіберзлочинністю МВС України, найбільш поширеними видами кіберзлочинів є: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів) та несанкціоновані дії з інформацією, яка ними оброблюється.

За 10 місяців 2012 р. зафіксовано 44 таких втручання. За даними Державної служби фінансового моніторингу України, у 2012 р. було зареєстровано 179 спроб несанкціонованого доступу до рахунків клієнтів банків на загальну суму понад 150 млн грн, при цьому сума коштів, у подальшому знятих злочинним шляхом лише готівкою, становить 9,5 млн грн [3, с. 282–283].

Як повідомила керівник Форуму безпеки платіжних операцій і кредитів Олеся Данильченко, 2013 р. охарактеризувався появою в Україні нового типу шахрайства з банкоматами – Transaction Reversal Fraud (TRF). Принцип його полягає у втручанні зловмисників у роботу банкомата в процесі видачі готівки за допомогою спеціального пристрою типу "вилка". Гроші при цьому знімаються з рахунку користувача, але банкоматом не видаються, а переправляються на інші джерела.

За даними міжбанківської системи протидії шахрайству, у 2013 р. українськими банками було зафіксовано 468 фактів несанкціонованого переказу коштів за допомогою систем дистанційного банківського обслуговування (ДБО). Станом на 10 січня 2014 р. в міжбанківському "чорному" списку одержувачів несанкціонованих платежів перебував 591 контрагент, дані про яких використовуються в локальних стоп-листах банків. Завдяки цьому списку банки мають можливість не тільки зупиняти відправку несанкціонованих платежів на користь цих одержувачів і затримувати зарахування їх вхідних платежів, а й відстежувати відкриття такими контрагентами нових рахунків і запобігати отриманню ними нових несанкціонованих платежів [7].

Поширений у зарубіжній літературі термін "кіберзлочинність" охоплює будь-який злочин, що вчиняється за допомогою комп'ютера, комп'ютерної системи з використанням глобальної мережі Інтернет, або проти комп'ютерної системи чи мережі. Цей термін охоплює такі види діянь, що зазвичай ви-

значаються як протиправні або найближчим часом можуть бути віднесені до кримінальних діянь.

Специфічна особливість глобальної мережі – відсутність кордонів. Обмін пропозиціями між членами злочинних угруповань можливий через анонімні поштові адреси, які закриваються після успішного завершення операції. Поширеним видом незаконного використання глобальної комп'ютерної мережі є несанкціоноване втручання в роботу автоматизованих систем телефонного зв'язку, що дає змогу безкоштовно користуватися послугами міжнародних телефонних переговорів. Але найнебезпечнішими злочинцями в кіберпросторі є професіонали, які використовують свої знання для промислового шпигунства, політичних цілей, тероризму [8, с. 45].

У складі злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку найбільшу небезпеку для суспільства, особи, держави становлять такі злочини, що мають ознаки організованої злочинності: комп'ютерний тероризм; диверсії, інші прояви антагоністичної інформаційної боротьби кримінальних формувань з державою, правоохоронними органами; крадіжки інформації з баз даних та комп'ютерних програм; шахрайства з використанням комп'ютерних технологій, особливо у сфері міжнародних економічних відносин (кредитно-фінансова, банківська) тощо [9, с. 56].

Найпоширеніші за способом вчинення є такі злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, як несанкціонований доступ до інформації в автоматизованих (комп'ютерних) системах. Поширення сучасних електронних засобів та простота їх управлінням породжує потенційні загрози подолання технічного захисту інформації в автоматизованих (комп'ютерних) системах, у тому числі таких, що становлять мережі телекомунікацій (окремих підприємств, галузевих, загальнодержавних, транскордонних). Це зумовлює потенційну об'єктивну й суб'єктивну недостатність технічної захищеності таких систем від несанкціонованого доступу, що становить соціогенну (зокрема криміногенну) загрозу. Крім того, виникають обставини, які зумовлюють ланцюгову реакцію щодо небажаного для конкретного суб'єкта суспільних інформаційних відносин несанкціонованого витоку інформації, її блокування (несанкціонованого обмеження доступу для правомірних користувачів інформації), спотворення (несанкціонованої модифікації) чи знищення інформації у комп'ютерній формі (комп'ютерної інформації) [10, с. 89].

Значного поширення з розвитком глобалізації інформатизації суспільства набуває таке соціальне явище, як хакерський рух – формування корпорацій осіб, які володіють ґрунтовними знаннями комп'ютерних технологій.

Відомо, що рівень злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку можна охарактеризувати за такими кількісними параметрами: скільки вчинено злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; скільки зареєстровано злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; скільки засуджено злочинців, які вчинили злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку характерні тим, що більшість із них неможливо виявити без використання спеціальних практичних заходів, особливо, на нашу думку, це стосується злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, пов'язаних із провайдерами та операторами зв'язку, а саме: несанкціонованого копіювання інформаційних файлів програм, несанкціонованого доступу до інформаційних масивів і баз даних в АС. Дійсно, зловмисник, здійснивши несанкціоноване копіювання інформації з жорсткого диску ЕОМ на гнучкий диск, тобто, здійснивши крадіжку інформації, практично не залишає слідів (у значенні фіксації своїх дій у комп'ютері). Це відбувається з тієї причини, що первісно операція копіювання інформації з диска на диск розроблялася як функціонально необхідна в ЕОМ, і тому не передбачалося жодних заходів з її авторизації.

Як спеціальні заходи, що перешкоджають реалізації злочинних намірів, використовують системи розмежування доступу (СРД) до ресурсів автоматизованих систем (програмні, програмно-апаратні й апаратні), які містять найрізноманітніші механізми захисту інформації в АС. Саме застосування таких систем дає змогу, як мінімум, фіксувати факт вчинення несанкціонованих дій узагалі у сфері діяльності комп'ютерних мереж, а також провайдерів та операторів зв'язку.

Практичний досвід свідчить, що на сьогодні, в умовах застосування недостатньо стійких (надійних) СРД, факт вчинення злочину у сфері використання електронно-

обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку в більшості випадків виявляється за вторинними наслідками, тобто за крадіжкою грошових коштів, інтелектуальної власності, здійсненням аварій, незаконним використанням інформації тощо. І навіть у цих випадках не всі потерпілі йдуть на те, щоб оприлюднити факт злочинних посягань на їхні комп'ютерні системи. Мотиви при цьому найрізноманітніші: від найлегковажніших, з посиланням на випадок, до побоювання втрати престижу фірми з метою запобігання втраті клієнтів.

Специфіка вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку визначає їх високу латентність. При цьому латентність, з урахуванням специфіки вчинення та фіксації злочинів, має природний характер. Штучної латентності, за ініціативою правоохоронних органів, практично немає, оскільки більшість "оприлюднених" злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку зазвичай мають високий суспільний резонанс, з іншого боку, власники комп'ютерних систем не поспішають сповіщати третіх осіб про успішні атаки на їхні системи.

Виходячи з особливостей злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, доцільно проводити окрему реєстрацію порушень у цій сфері, оскільки кількість злочинів або спроб їх вчинення, зареєстрованих власниками автоматизованих систем, значно перевищує кількість таких злочинів, зареєстрованих правоохоронними органами [11, с. 13–14].

У США, де найбільш гостро відчувають проблему комп'ютерної злочинності, намагаються побудувати розгалужену систему боротьби з нею. У ФБР створено Центр комп'ютерних злочинів і оцінювання загрози інфраструктури (Computer Investigation and Infrastructure Threat Assessment Centr). Сама назва Центру говорить про спрямування його роботи. Незважаючи на те, що Центр існує не так давно, він уже зараз отримав широкі повноваження щодо контролю за найбільш вразливими складовими інформаційної інфраструктури держави: фінансовою системою, телефонною мережею, управлінням рухом, управлінням енергосистемою тощо.

IV. Висновки

Співпраця у сфері боротьби з "картковою" злочинністю має бути спрямована на розробку та реалізацію конкретної програми, яка повинна включати такі заходи: навчання слідчих органів, прокуратури й судових органів методів та особливостей боротьби з фінансовими махінаціями у сфері високих інформаційних технологій, у тому числі у сфері платежів із застосуванням платіжних карток; посилення підрозділів правоохоронних органів, органів кримінальної експертизи та суду, відповідальних за провадження справ, пов'язаних з махінаціями з кредитними картками; поліпшення взаємодії між банками, комерційними структурами й правоохоронними органами з питань боротьби з фінансовими махінаціями, розробка та запровадження в банках України заходів щодо оперативного виявлення й запобігання злочинним операціям з платіжними картками; створення Єдиної інформаційної бази банків з метою антишахрайства обміну інформацією (спільні дії НАБУ, НБУ та правоохоронних органів), що надасть можливість запобігти типовим схемам кібератак, мінімізувати наслідки виявлених нападів, відстежити слабкі й найменш захищені місця в системах інформаційного захисту банків; удосконалення законодавства України стосовно "карткових" та злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Ефективна співпраця з іноземними уповноваженими органами має здійснюватися за напрямами: розробки та впровадження (законодавчого закріплення) спрощених механізмів оперативного обміну інформацією щодо фінансових операцій з ознаками зловживань або підробок кредитних карток, у тому числі для цілей легалізації "брудних" капіталів, ідентифікації осіб, причетних до їх проведення; обміну позитивним досвідом роботи у сфері боротьби з фінансовими махінаціями з правоохоронними й контролюючими органами іноземних держав, проведення спільних конференцій з питань забезпечення "прозорості" фінансових операцій, створення умов для ефективної боротьби правоохоронних та інших уповноважених державних органів з фінансовими махінаціями й легалізацією "брудних" доходів; організації спеціальної системи підготовки фахівців правоохоронних і фінансово-банківських структур України на базі відповідних навчальних закладів країни зі значним практичним досвідом протидії злочинам з використанням пластикових платіжних засобів.

Список використаної літератури

1. Борисова Л.В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : дис. … канд. юрид. наук : 12.00.09 [Електронний ресурс] / Л.В. Борисова ; Київський національний ун-т внутрішніх справ. – К., 2007. – 217 арк. – Режим доступу: http://www.lib.ua-ru.net/diss/cont/243813.html.

2. Телійчук В.Г. Захист та безпека інформації в роботі оперативних підрозділів як складова національної безпеки держави / В.Г. Телійчук // Національні інтереси та проблеми забезпечення безпеки України : матеріали всеукр. наук.-практ. конф., м. Кіровоград, 18–19 листопада 2010 р. / за заг. ред. В.П. Пєткова. – Кіровоград : Кіровоградський юрид. ін-т ХНУВС, 2009 – С. 184–186.
3. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку [Електронний ресурс]. – Режим доступу: http://www.scourt.gov.ua/clients/vs.nsf/0/C8EABE11C12BFF3AC22576EE004F1E65?.
4. Телійчук В.Г. Способи вчинення комп'ютерних злочинів у сфері високих технологій та заходи протидії / В.Г. Телійчук // Актуальні питання юридичної науки: теорія та практика : матеріали міжнар. наук.-практ. конф., м. Кіровоград, 11 грудня 2013 р. / Кіровоградський ін-т. держ. та муніц. упр. КПУ. – Кіровоград : КІДМУ КПУ, 2013. – С. 281–284.
5. Савор О.В. Комп'ютерна злочинність в Україні та за кордоном / О.В. Савор // Взаємодія правоохоронних органів з провайдерами та операторами зв'язку в боротьбі з комп'ютерними злочинами : матеріали регіонального наук.-практ. семінару, м. Донецьк, 12 грудня 2008 р. / Донецький юрид. ін-т ЛДУВС ім. Е.О. Дідоренка. – Донецьк : ДЮІ ЛДУВС, 2009. – С. 109–113.
6. Телійчук В.Г. Протидія злочинам, що вчиняються організованими злочинними угрупованнями з використанням комп'ютерних технологій / В.Г. Телійчук // Організація і тактика документування підрозділами ДСБЕЗ злочинів у комп'ютерних мережах та мережах електрозв'язку" : матеріали всеукр. наук.-практ. конф., м. Донецьк, 4 грудня 2009 р. / Донецький юрид. ін-т ЛДУВС ім. Е.О. Дідоренка. – Донецьк : ДЮІ ЛДУВС, 2009. – С. 198–202.
7. Обережно – кіберзлодії! [Електронний ресурс]. – Режим доступу: http://anticyber.com.ua/article_detail.php?id=196.
8. Голубєв В.О. Конвенція щодо боротьби з кіберзлочинністю як елемент правового механізму взаємодії правоохоронних органів із провайдерами у боротьбі з комп'ютерними злочинами / В. О. Голубєв // Взаємодія правоохоронних органів з провайдерами та операторами зв'язку в боротьбі з комп'ютерними злочинами : матеріали регіонального науково-практичного семінару, м. Донецьк, 12 грудня 2008 р. / Донецький юрид. ін-т ЛДУВС ім. Е.О. Дідоренка. – Донецьк : ДЮІ ЛДУВС, 2009. – С. 43–48.
9. Злобін Д.Л. Взаємодія операторів мобільного зв'язку з ОВС при розслідуванні комп'ютерних злочинів / Д.Л. Злобін // Взаємодія правоохоронних органів з провайдерами та операторами зв'язку в боротьбі з комп'ютерними злочинами : матеріали регіонального наук.-практ. семінару, м. Донецьк, 12 грудня 2008 р. / Донецький юрид. ін-т ЛДУВС ім. Е.О. Дідоренка. – Донецьк : ДЮІ ЛДУВС, 2009. – С. 56–61.
10. Поливода О.Ю. Боротьба з комп'ютерною злочинністю в Україні: проблемні питання / О.В. Поливода // Взаємодія правоохоронних органів з провайдерами та операторами зв'язку в боротьбі з комп'ютерними злочинами : матеріали регіонального наук.-практ. семінару, м. Донецьк, 12 грудня 2008 р. / Донецький юрид. ін-т ЛДУВС ім. Е.О. Дідоренка. – Донецьк : ДЮІ ЛДУВС, 2009. – С. 88–91.
11. Бєлєй К.В. Актуальні проблеми виявлення латентних комп'ютерних злочинів / К.В. Бєлєй // Взаємодія правоохоронних органів з провайдерами та операторами зв'язку в боротьбі з комп'ютерними злочинами : матеріали регіонального наук.-практ. семінару, м. Донецьк, 12 грудня 2008 р. / Донецький юрид. ін-т ЛДУВС ім. Е.О. Дідоренка. – Донецьк : ДЮІ ЛДУВС, 2009. – С. 12–16.

Стаття надійшла до редакції 23.05.2014

Телийчук В.Г. Способы совершения преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей, сетей электросвязи и меры противодействия

В статье рассмотрены способы совершения преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи, определено распределение преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи по типам. Исследовано совершение указанных преступлений организованной преступностью, которая определяется высокой вероятностью социальной опасности, сложностью выявления, установления вины и сбора доказательств. Определены особенности совершения преступлений в сфере использования электронно-вычислительных машин (компьюте-

ров), систем и компьютерных сетей и сетей электросвязи организованными преступными группами. Обращено внимание на совершение указанных преступлений в банковской сфере, определены основные способы совершения. Проведено исследование статистических показателей совершения указанных преступлений за последние два года, характеризующиеся появлением в Украине нового типа мошенничества с банкоматами. Определены меры противодействия преступлениям в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи.

Ключевые слова: *транснациональные преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи, преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи, криминалистика, оперативно-розыскная деятельность, преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи, совершаемых организованной преступностью, способы совершения преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи, совершаемых организованной преступностью, особенности совершения преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи, совершаемых организованной преступностью, системы разграничения доступа, сотрудничество в сфере борьбы с "карточной" преступностью.*

Teliychuk V. Methods of committing crimes in the sphere of the use of E-computers (computers), computer systems and networks, elektrosvyazi and Countermeasures

The article discusses ways of committing crimes in the use of computers (PCs), systems and computer networks and telecommunication networks, distribution defined crimes in the use of computers (PCs), and computer systems' computer networks and telecommunication networks by Type. To commit such crimes are investigated organized crime, which is determined by a high probability of social danger, the complexity of identifying, establishing guilt and evidence gathering.

Defined features of committing computer crimes by organized criminal groups, where the mandatory presence of such a specific participant criminal group as a hacker (Fricker, crackers and the like). Author drew attention to the fact that this slang term refers to the person who owns the knowledge and skills of unauthorized entry into a computer system. It is the main executor of the crime.

Two main types of computer crimes to the first, are crimes in which the object of their implementation have computers: neutralization or replace data, software and hardware; theft of input, output, software and hardware; economic espionage and disclosure of information constituting a state or commercial secrets; other criminal acts of this kind, to the second, illegal actions, the implementation of which computers are used as tools in achieving the criminal objective: computer sabotage; Extortion and blackmail embezzlement; embezzlement of funds; deception of consumers, investors or users; other crimes. The category of "other criminal acts" attributed unauthorized use of a computer for personal use.

The author defines the concept of computer crime under which it should be understood socially dangerous act (act or omission) that is carried out using modern information technology and computer technology with the aim of causing damage to property or to the public interest of the state, businesses, agencies, organizations of various forms of ownership, public formation and citizens, as well as human rights.

Besides, the author points to the commission of the above crimes in the banking sector, the basic ways of committing, highlighted by the most common method of execution. We investigate the statistical indicators of committing computer crimes over the past two years, characterized by the appearance in Ukraine of a new type of ATM fraud. The principle of which is meddling intruders in ATM operation in the process of issuing cash with a special device such as " fork."

Characterized by the level of computer crime in its quantitative indicators. Defined countermeasures computer crimes.

Key words: *transnational crimes in the use of computers (PCs), systems and computer networks and telecommunication crimes in the use of computers (PCs), systems and computer networks and telecommunication networks' communication, forensics, operational-search activity, crime in the use of computers (PCs), systems and computer networks and telecommunication networks organized crime committed, the methods of committing crimes in the use of computers (PCs), systems and computer networks and telecommunication networks committed organized crime, particularly the commission crimes in the use of computers (PCs), systems and computer networks and telecommunication networks that organized crime committed, access control systems, cooperation in the fight against "card" crime.*