УДК 343.98.06

Самойленко Олена Анатоліївна –
кандидат юридичних наук, доцент кафедри кримінального права та процесу Донецького національного університету

Сутність викрадень майна, вчинених із використанням комп'ютерних технологій

У статті проаналізовано емпіричні дані щодо викрадення майна, вчиненого із використанням комп'ютерних технологій, організованими угрупованнями, розглянуто структуру ОЗГ, що має важливе значення для розслідування зазначеної категорії деліктів.

Ключові слова: викрадення майна, комп'ютерні технології, організовані злочинні угруповування, організована злочинність.

Результати науково-технічного прогресу створюють надзвичайно досконалі можливості для вчинення як невідомих раніше правопорушень (передбачених ст.ст. 361 – 363–1 КК України), так і традиційних злочинів новими засобами. Тому сьогодні для України є актуальним дослідження таких проблемних питань методики розслідування, як вплив комп'ютерних технологій на криміналістичну характеристику традиційних видів злочинів, зокрема формування слідчих ситуацій, тактику проведення слідчих дій під час розслідування викрадення майна. Адже аналіз даних Департаменту інформаційних технологій при МВС України щодо кількості кримінальних справ, порушених за ознаками комп'ютерного злочину по регіонах України свідчить, що сьогодні 90 % таких справ – це злочини проти власності.

У той же час у дослідженнях П.Д. Біленчука, В.О. Голубєва, М.В. Гуцалюка, О.М. Моїсєєва, Л.П. Паламарчук, М.В. Салтевського та інших криміналістів приділяється увага розслідуванню комп'ютерних злочинів, але без урахування зв'язку зі злочинами проти власності та економічними злочинами. Автори ж, які досліджували проблематику розслідування економічних злочинів (А.Ф. Волобуєв, Г.А. Матусовський, П.В. Мельник та інші), розглядали лише окремі аспекти використання злочинцями комп'ютерних технологій. На практиці ж правоохоронні органи продовжують стикатися з низкою труднощів під час розслідування таких викрадень, що пов'язано з незнанням працівниками їх сутності та механізмів учинення. Саме це безпосередньо впливає на якість проведення окремих слідчих дій, оперативно-розшукових та організаційних заходів під час розслідування викрадень майна, вчинених із використанням комп'ютерних технологій.

Сутність викрадень майна, вчинених з використанням комп'ютерних технологій, полягає в тому, що ці злочини являють собою дії по заволодінню чужим майном під час якого комп'ютер (комп'ютерна система, мережа) використовується як необхідний технічний засіб для вчинення цих дій. Поряд з цим викрадення майна за допомогою комп'ютерної техніки вчиняються, перш за все, в банківській та підприємницькій сфері, де обертаються величезні кошти у безготівковій формі та операції з ними здійснюються з використанням електронних засобів.

Базуючись на матеріалах кримінальних справ, можна виділити наступні різновиди (механізми) викрадень майна, вчинених з використанням комп'ютерних технологій.

1. Переведення коштів з банківських рахунків клієнтів банку оператором банку чи іншою службовою особою на рахунки комерційних структур або фізичних осіб з подальшим їх зняттям готівкою. Саме такий вид викрадення найчастіше виявляється правоохоронними органами України. Один з перших таких злочинів зареєстровано у 1994 р. Так, у червні в Дніпропетровській області було припинено спробу викрадення 864 млн крб. Ведучий інженер-комп'ютерник регіонального управління Промінвестбанку м. Дніпропетровська Т. проник до комп'ютерної мережі банку через власний комп'ютер за допомогою заздалегідь скопійованої системи захисту комп'ютерної системи банку, після чого незаконно здійснив фінансову операцію з корисливою метою. Сьогодні такі злочини вчиняють не лише банківські працівники, а й посадові особи підприємств різних форм власності. Так, з 27 жовтня по 11 грудня 2003 р. головний бухгалтер ТОВ "Б" гр. В. шляхом виготовлення підроблених платіжних доручень на перерахування грошей, використовуючи програмно-технічний комплекс електронних розрахунків "Банк-Кліент" з грошового рахунку ТОВ у Каховському відділенні банку "Аваль" перерахував 15 274 грн на рахунок власного ПП у Каховському відділенні КБ "Приватбанк".

2. Переведення коштів з банківських рахунків "хакером" на рахунок комерційної установи. Ця група злочинів відрізняється від вищенаведеної лише особою злочинця, бо суб'єкт вчинення злочину є спільним. В Україні зареєстровано поодинокі випадки таких викрадень. Незважаючи на це, у конфіденційних джерелах електронних платежів НБУ щоденно в середньому "відбивається" близько 20–30 спроб несанкціонованого проникнення ззовні [1, с. 249]. СБУ зафіксовано спроби несанкціонованого доступу до комп'ютерної мережі Укрексімбанку шляхом втручання в його роботу через мережу Інтернет.

3. Отримання коштів за банківськими пластиковими картками, які були заздалегідь скопійовані або викрадені у власника (шахрайські дії з пластиковими платіжними засобами). Так, у червні 2003 року Печерським районним судом м. Києва було засуджено гр. Г. за вчинення злочинів, передбачених ст.ст. 190 (ч. 3), 200 (ч. 2), 358 (ч. 2), 358 (ч. 3) КК України, до 3-х років позбавлення волі. Слідством було встановлено, що у грудні 2002 року в м. Києві гр. Г., використовуючи підроблену пластикову картку на ім'я гр. України Я., вісім разів здійснив розрахування за придбані ним речі в різних торговельних точках м. Києва. Факти вчинення таких злочинів набули широкого розповсюдження з початку 2003 р., їх було зареєстровано в Одеській, Львівській, Харківській, Донецькій та інших областях України. Але слід звернути увагу на одну з особливостей такого злочину, а саме: до кримінальної відповідальності за вказаний злочин, як правило, притягується особа, яка використовувала таку картку, а не виготовила її самостійно – виробники ж карток, які становлять особливу суспільну небезпеку, залишаються невстановленими в ході слідства. Так, нещодавно за сприяння НЦБ Інтерполу в Україні комендатурою муніципальної поліції Польщі при спробі розрахуватися підробленими платіжними картками в торгівельній мережі на території Польщі були затримані громадяни України Г. та Д., які були членами організованої злочинної групи у м. Бровари Київської області. До обов'язків Г. та Д. входило шахрайське використання підроблених банківських карток у магазинах Польщі та відправка придбаного таким чином товару в Україну з метою його подальшої реалізації у магазинах. Цей вид шахрайства характеризує відносна простота, відсутність насилля, а також та обставина, що ні банк, ні законний володар картки, як правило, ніколи не бачать злочинця. Треба зазначити, що існує безліч модифікацій злочинів цієї групи залежно від конкретних елементів криміналістичної характеристики.

4. Заволодіння чужими коштами під час укладення договорів купівлі-продажу через Інтернет. Сьогодні в світі нараховується понад 30 видів незаконних операцій з пластиковими картками або різновидом електронної готівки – електронними

монетками (cidercash) – через мережу Інтернет: оплата неіснуючими картками, створення фальшивих віртуальних магазинів, фальшиві оплати в ігорних установах тощо [2, с. 12]. Сенс у тому, що злочинець за певну послугу або товар розплачується, вказуючи номер певної кредитної картки. Ці номери карток хакер може отримати як самостійно, так і через іншу людину. Наприклад, після затримання зловмисника у нього було вилучено код для доступу до інформації про номери карток "Viza AeroGold". У розпорядженні хакера перебувало 315 діючих номерів кредитних карток, отриманих за допомогою комп'ютера, без використання традиційних способів викрадання. На деяких таємних дошках електронних оголошень в комп'ютерних мережах можна зустріти рекомендації про способи вчинення шахрайства з використанням кредитних карток. Тож, вищезгадані номери карток в електронному вигляді злочинець може придбати у такого хакера або отримати інформацію про механізм вчинення злочину через таку дошку оголошень. Подібні злочини, як свідчить практика, зареєстровані в країнах, які мають розвинуті комп'ютерні технології, насамперед у США. За оцінками Рахункової палати Уряду США, щорічний збиток для власників магазинів від викрадень і шахрайств, учинених за допомогою інформаційних технологій тільки через Інтернет, становить понад 5 млрд дол. США [3, с. 84]. Правоохоронними органами України цей вид злочину реєструється поодиноко, що свідчить про високий рівень його латентності, а не про відсутність, оскільки ще в березні 2001 року Федеральна служба безпеки спеціально попереджувала американські компанії про загрозу з боку хакерів, головним чином з Росії та України [4]. До того ж, за даними американського Федерального бюро розслідувань, за кілька місяців 2001 р. було розкрито "ряд організованих груп хакерів із Західної Європи, насамперед із Росії та України" [5, с. 161]. Дійсно для українських злочинців інтерес становлять саме закордонні електронні магазини, оскільки в Україні ця галузь суспільної діяльності ще не досить розвинута – в їх асортименті немає цінних товарів.

Це дає підстави для висновку, що з криміналістичної точки зору викрадення, вчинені з використанням комп'ютерних технологій, є не одиничним злочином, а сукупністю різних, але взаємопов'язаних однією корисливою метою. Тому коло таких злочинців нічим не обмежується – це може бути банкір, народний депутат, підприємець, спеціаліст високого класу у сфері комп'ютерних технологій, звичайний кишеньковий крадій тощо. Це дає підстави вести мову про організований характер цієї злочинної діяльності. Якщо за кримінальною справою звинувачують у вчиненні злочину лише одну особу, то можна вважати, що порушується принцип повноти та всебічності в розкритті злочинів, адже для безпосереднього використання безготівкових коштів, якими заволодів злочинець, необхідно звернутися хоча б до механізму легалізації незаконно отриманого прибутку.

Поряд з цим за даними МВС України можна зробити висновок, що із 100 % виявлених викрадень, учинених із використанням комп'ютерних технологій, лише 5–10 % учинялися групою осіб. На нашу думку, такий показник повинен складати хоча б 50–60 % із 100 %. У підтвердження цього висловлювався ще у 1996 році В.Б. Вєхов, вважаючи, що 62 % злочинців учиняли злочини у сфері комп'ютерної інформації в складі злочинних угруповань [6, с. 37].

Організована злочинна група (ОЗГ) існує як багаторівнева система, що складається з різних ланок. Основним принципом організації таких груп є ієрархічність та обов'язкова наявність організатора, місце якого визначається на основі якостей, притаманних його особистості.

Залежно від способу викрадання до складу ОЗГ входять: організатори (1 група); працівники обліку та контролю – бухгалтери, працівники грошових кас або відділів банку, що контролюють платежі, та ін. (2 група); керівники власних комерційних структур, їх бухгалтери або особи, які виконують їхню роль (3 група); рядові виконавці (4 група); окремо слід відзначити "злочинців-інтелектуалів", які

використовують свої професійні навички роботи з комп'ютерною технікою [7, с. 26]. "Злочинець-інтелектуал" (хакер) може "підключатися" на будь-якому етапі вчинення злочину чи бути його безпосереднім організатором. Звернемо увагу, що інформація щодо безлічі підпільних організацій хакерів не стосується викрадень за допомогою комп'ютерної техніки організованою групою [8, с. 26].

Перша та друга групи можуть у деяких випадках об'єднуватися, оскільки організатором часто буває керівна особа потерпілої установи, до повноважень якої належить гарантування безпеки грошових операцій. Як відзначається в деяких юридичних джерелах, необхідно відмітити вагомий показник керівних працівників, які вчинили викрадення з використанням комп'ютерної техніки в складі ОЗГ (35 %). Зокрема, це стосується працівників банківських структур, адже за 2005–2006 роки в Україні викрито чотири ОЗГ, у складі яких були працівники банків [9]. Це обумовлено тим, що керівником, як правило, є фахівець більш високого класу, який володіє професійними знаннями та має право віддавати розпорядження й накази виконавцям, але безпосередньо не відповідає за роботу засобів комп'ютерної техніки. Організатор злочину – це, передусім, особа, спроможна забезпечити діяльність усіх учасників групи, а також, яка володіє достатніми знаннями для того, щоб правильно побудувати ланцюг зв'язків членів групи та помірковано підійти до планування етапів учинення злочину.

До третьої групи належать особи, на ім'я яких або на рахунок підприємства яких будуть перераховані викрадені з використанням комп'ютерної техніки шляхом зняття з банківського рахунку чужі гроші. Такі особи повністю залежать від організатора злочину, можуть мати вищу та незакінчену вищу освіту, бути судимими за вчинення економічних злочинів. У випадку, якщо вказаних осіб насправді не існує, а вони є вигаданими або вже померли, то за цим обов'язково "стоїть" організатор такого злочину.

Дуже специфічною є четверта група. Якщо говорити про викрадення, вчинене шляхом шахрайства з використанням викраденої або загубленої картки, то крадіжки пластикових засобів вчинюють повії, викрадачі з кишень, викрадачі з квартир, працівники пошти та ін. Ці особи або їх посередники, не маючи достатніх знань для їх використання в злочинних цілях, збувають викрадені картки (або їх сліпи) працівникам сервісних підприємств. Виконавці використовуються також для завершення злочину – зняття з підробленої або викраденої картки грошей у банкоматі або використання її в магазині під час оплати придбаного товару. Крім того, багатьом з них "немає чого втрачати": особа може мати декілька судимостей, бути хворою на наркоманію або алкоголізм чи не мати постійного місця проживання.

Наведені положення можна проілюструвати прикладом із практики [10]. У кінці серпня 2002 року гр. Ш., виконуючи службові обов'язки офіцера податкової міліції, звернувся до свого знайомого гр. Г., який працював інженером-програмістом у Бахмацькій автомобільній школі та мав у розпорядженні власний комп'ютер, з пропозицією про вчинення крадіжки великої суми грошей за допомогою комп'ютерної техніки. Для цього на гр. Г. було покладено обов'язок залучити до групи з кола знайомих програмістів особу, яка має доступ до електронних платежів у зв'язку з роботою в установі, що стане жертвою. У свою чергу гр. Г. звернувся до К., який працював інженером-програмістом Бахмацького відділення ВАТ "Державний Ощадний банк України". У результаті цілеспрямованого впливу К., який мав доступ до здійснення електронних платежів, що проводив зазначений банк, дав згоду на участь у викраденні грошей із названого банку. Таким чином, на початку жовтня 2002 року було створено ОЗГ, членами якої були громадяни Ш., Г., К. При цьому гр. Ш. здійснював загальне керівництво членами групи та розробив план вчинення злочину, саме він зголосився підшукати фірму, на яку повинні були перерахувати викрадені гроші; квартиру, обладнану телефонним зв'язком, з якої здійснювалося

перерахування грошей; організувати переведення безготівкових викрадених грошей у готівку і за винятком затрат, необхідних для їх обернення в готівку, поділити між учасниками групи. На гр. Г. покладались обов'язки надати комп'ютер з модемом, необхідний для здійснення електронного платежу, та допомагати гр. К. у здійсненні незаконного переказу. Гр. К. повинен був скопіювати на вінчестер комп'ютера, який надасть йому гр. Г., програми зі здійснення електронних платежів указаним Ощадбанком, а також на флопі-диск секретний ключ для їх запуску, після чого винести їх з приміщення банку та встановити на комп'ютері гр. Г. і, запустивши банківські програми зі здійснення електронних платежів, разом з гр. Г. набрати необхідні платежі та відправити їх в електронному вигляді на рахунок фірми, наданий їм гр. Ш., у день викрадення грошових коштів.

Виконавши необхідні приготування, 16 жовтня 2002 року о 9 годині ранку гр. К. у приміщенні Бахмацького відділення Ощадбанку після запуску програми зі здійснення платежів скопіював на вінчестер програми зі здійснення електронних платежів банку, ключ до них та виніс їх із приміщення. Після цього гр. К. на автомобілі під керуванням знайомого гр. А. (причетність його до вчинення вищезазначеного злочину слідством не було встановлено) прибув до будинку, що належав знайомим гр. Ш., причетність яких також не було встановлено. Перебуваючи в будинку, до якого за розробленим планом прибув гр. Г., а через деякий час і гр. Ш., члени організаційної групи встановили комп'ютерне обладнання та запустили банківські програми за допомогою викраденого секретного коду, наладнавши їх на режим автоматичного переказу грошових коштів. У перебігу цього гр. К. разом із гр. Г. набрали в електронному вигляді 17 платежів на перерахування 265 127 грн 45 коп. та 3 платежі на перерахування 200 000 грн. з Ощадбанку на рахунок приватного підприємства, наданого гр. Ш. При цьому перша сума була автоматично знята з кореспондентського рахунку банку, а інша заблокована системою захисту банку, оскільки перебувала за межами залишку кореспондентського рахунку. Інформацію про здійснення платежів гр. К. отримав уже на своєму робочому місці.

Під час допитів громадяни Г. та К. наголошували на тому, що гр. Ш. втягнув їх у злочинну групу, використовуючи погрози фізичною розправою, і вони навмисно здійснили останній платіж, підозрюючи, що той буде зупинений службою охорони банку. Однак слідством було доведено, що останні мали реальну можливість відмовитися від вчинення злочину, але не зробили цього. Гр. Ш. як організатора було засуджено за ст. 27 (ч.3), ст. 191 (ч. 5); ст. 27 (ч. 3), ст. 15 (ч. 2,) ст. 191 (ч. 5); ст. 27 (ч.3), ст. 28 (ч. 3), ст. 200 (ч. 2); ст. 27 (ч. 3), ст. 28 (ч. 3), ст. 232; ст. 27 (ч. 3), ст. 28 (ч. 3), ст. 362 (ч. 3) КК України. За аналогічними статтями засуджені громадяни Г. та К.

Базуючись на результатах вивчення кримінальних справ, можна зазначити, що для заволодіння грошима шляхом перерахування їх з одного рахунку банку на інший за ознакою стійкості злочинної спрямованості такі групи створюються як тимчасове об'єднання на період вчинення конкретного злочину. Для вчинення ж злочинів шляхом використання підроблених платіжних банківських карток або через укладення договорів купівлі-продажу в Інтернет-мережі створюється стійке організоване злочинне угруповання. Доцільно також відмітити певні риси, притаманні ОЗГ щодо викрадення майна, вчиненого з використанням комп'ютерних технологій: а) формування груп відбувається змішано: формально наявні виробничі (службові) та особисті (нетрудові) зв'язки; б) групи за способами утворення формуються як добровільні об'єднання, в окремих випадках – шляхом активного втягування в групу організатором потрібних за посадою осіб.

Таким чином, систематизована інформація про структури ОЗГ, розподіл ролей між співучасниками, їх методів втягування у злочинну діяльність інших осіб має важливе значення для розслідування викрадень майна, вчинених із використанням

комп'ютерних технологій, та потребує постійного дослідження з урахуванням модернізацій відомих способів вчинення викрадення.

Список використаних джерел

1. *Цимбалюк В.С.* Кримінологічні аспекти вчинення правопорушень у сфері міжнародних економічних відносин із застосуванням інформаційних комп'ютерних технологій / В.С. Цимбалюк // Збірник наукових праць Харківського центру з виявлення організованої злочинності спільно з Американським університетом м. Вашінгтон. – 2002. – № 6. – С. 234–260.
2. *Гуцалюк М.В.* Пластиковый бизнес в Украине или особенности национального мошенничества / М.В. Гуцалюк // Бизнес и Безопасность. – 2001. – № 2. – С. 9–12.
3. *Смаглюк О.* Шахрайство, вчинене шляхом незаконних операцій з використанням обчислювальної техніки / О. Смаглюк // Підприємництво, господарство та право. – 2002. – № 6. – С. 82–86.
4. *Селик Ю.*, Прохоров А. Internet – отмычка для комп'ютера / Ю. Селик, А. Прохоров // Компьютер-пресс. – 2002. – № 3. – С. 41.
5. *Загіка Г.В.*, Погрібний О.О. Особливості боротьби з комп'ютерною злочинністю / Загіка Г.В. // Вісник Одеського університету внутрішніх справ МВС України. – 2002. – № 4. – С. 160–163.
6. *Вехов В.Б.* Компьютерные преступления: Способы совершения и раскрытия / Вехов Виталий Борисович; [под ред. Б.П. Смагоринского]. – М.: Право и Закон, 1996. – 182 с.
7. *Луценко О.А.* Расследование хищений в сфере банковской деятельности: науч. – практ. пособие / О.А. Луценко. – Ростов н/Д.: Рост. ун-т, 1998. – 140 с.
8. *Біленчук П.Д.*, Котляревський О.І. Портрет комп'ютерного злочинця: навч. посібник / П.Д. Біленчук, О.І. Котляревський. – К.: В & В, 1997. – 48 с.
9. *Матеріали* відділу боротьби з правопорушеннями у сфері високих технологій ДДСБЕЗ МВС України оголошено на конференції з питань міжнародної співпраці згідно з положеннями Конвенції Ради Європи про кіберзлочинність у межах проекту міжнародного співробітництва у сфері кримінальних справ в Україні, яка відбулася 6-7 лютого 2007 р. у м. Києві у Секретаріаті Ради Європи.
10. *Кримінальна* справа за № 1-123 за 2003 р. / Архів місцевого суду Бахмацького району Чернігівської області.

В статье проанализированы эмпирические данные о хищении имущества, совершенном с использованием компьютерных технологий организованными группировками, рассмотрена структура ОПГ, что имеет важное значение для расследования указанной категории деликтов.

The article is devoted to the analysis of the empiric information in relation to the theft of property committing with computer technologies by the organized group, the structure of organized criminal group is considered, which has an great importance for the investigation of this category of delicts.

Стаття надійшла до редакції журналу 21 травня 2009 року.

© О.А. Самойленко, 2009