МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
ДЕПАРТАМЕНТ КАРНОГО РОЗШУКУ

РОЗСЛІДУВАННЯ ШАХРАЙСТВ, УЧИНЕНИХ З ВИКОРИСТАННЯМ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

Методичні рекомендації

Київ

2021

УДК 343.985: 343.52 : 004] (072)
Р-754

Авторський колектив:

Коршикова Т. В., доктор філософії у галузі «Право» (Головне управління Національної поліції у м. Києві); ***Стрільців О. М.,*** кандидат юридичних наук, старший науковий співробітник (НАВС); ***Пархоменко Ю. О.,*** кандидат юридичних наук (Департамент карного розшуку Національної поліції України); ***Василинчук В. І.,*** доктор юридичних наук, професор (НАВС); ***Ніколенко О. С.,*** заступник начальника відділу (Департамент карного розшуку Національної поліції України); ***Тарасенко О. С.,*** кандидат юридичних наук, доцент (НАВС); ***Арешонков В. В.,*** доктор юридичних наук, старший науковий співробітник (НАВС); ***Куций Р. В.,*** кандидат юридичних наук (НАВС); ***Іванчук Н. В.,*** кандидат юридичних наук (НАВС); ***Павленко Н. Г.,*** кандидат юридичних наук, старший науковий співробітник (НАВС); ***Паламарчук К. В.,*** кандидат юридичних наук (НАВС); ***Федоренко О. А.*** (НАВС).

Рецензенти:

Окушко А. В. – заступник начальника управління – начальник відділу Департаменту кіберполіції Національної поліції України, кандидат юридичних наук;

Швець М. Я. – провідний науковий співробітник наукової лабораторії з проблем протидії злочинності навчально-наукового інституту № 1 Національної академії внутрішніх справ, доктор економічних наук, професор, заслужений діяч науки і техніки України.

Рекомендовано до друку науково-методичною радою Національної академії внутрішніх справ від 23 грудня 2021 року (протокол № 4)

Р-754 Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : метод. рек. / Коршикова Т. В., Стрільців О. М., Пархоменко Ю. О. Київ : Нац. акад. внутр. справ, 2021. 81 с.

У методичних рекомендаціях надано криміналістичну характеристику шахрайств, учинених з використанням електронно-обчислювальної техніки (предмет злочинного посягання, слідові картина та обстановка, особа злочинця та особа потерпілого), розкрито напрями уповноважених осіб правоохоронних органів під час попередження, припинення та розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки, а також особливості проведення окремих слідчих-розшукових дій та використання спеціальних знань під час розслідування кримінальних правопорушень вказаної категорії.

Призначено для працівників практичних підрозділів, слідчих, працівників інших правоохоронних органів України, а також для здобувачів вищої освіти закладів вищої освіти МВС України.

УДК 343.985: 343.52 : 004] (072)
© Національна академія внутрішніх справ, 2021,
Коршикова Т. В., Стрільців О. М., Пархоменко Ю. О. та ін.

ПЛАН

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ДНДЕКЦ	Державний науково-дослідний експертно-криміналістичний центр
ЄДРСР	Єдиний державний реєстр судових рішень
ЄРДР	Єдиний реєстр досудових розслідувань
ЕОТ	електронно-обчислювальна техніка
КПК	Кримінальний процесуальний кодекс
МВС	Міністерство внутрішніх справ
НП	Національна поліція
НСРД	негласні слідчі (розшукові) дії
ПВСУ	Пленум Верховного Суду України
СОГ	слідча оперативна група
СРД	слідча (розшукова) дія

ВСТУП

Можливості електронно-обчислювальної техніки та Всесвітньої мережі Інтернет безмежні та її використання відіграє все більшу роль у політичних, економічних та соціальних процесах в Україні та світі. Близько 78% населення України у віці 16 років та старше (приблизно 25 млн осіб) користується Інтернетом, при цьому покупки через Інтернет здійснюють понад 11 млн українців, з них кожний четвертий робить понад 20 замовлень на рік. Поряд з цим зростають негативні тенденції у суспільстві, здійснюються якісні та кількісних зміни кіберзлочинності, яка набуває все більш професійного, організованого та витонченого характеру. Через велику популярність онлайн-шопінгу збільшилася й активність онлайн-шахраїв. За статистикою ресурсу OLX Україна, частка шахрайств лише в онлайн-шопінгу з використанням сайтів-підробок становить близько 0,4% від усіх транзакцій, а за даними Української міжбанківської асоціація членів платіжних систем ЄМА[1] за допомогою Інтернет-мережі шахраї «заробили» 252 млн грн.

Як наслідок, лише у 2020 році до підрозділів кіберполіції Національної поліції України надійшло понад 33 тис. звернень (повідомлень) громадян стосовно шахрайський дій щодо них, вчинених у мережі Інтернет[2]. Найбільш розповсюдженими схемами вчинення шахрайств були продаж неіснуючих товарів на платформах оголошень або у соціальних мережах, а також використання фішингових ресурсів, які ззовні схожі на популярні Інтернет-магазини, банківські установи або організації. Також у 2020 році набули популярності шахрайські схеми, замасковані під сервіси доставки платформ оголошень.

Вказане ставить перед наукою завдання спрямовані на розробку новітніх прийомів, методів та засобів розслідування шахрайств, вчинених з використанням ЕОТ. У цьому контексті важливим є узагальнення наукових ідей і підходів до створення якісно нового механізму розслідування вказаних кримінальних правопорушень. Вказане спонукає до необхідності проведення комплексного наукового дослідження розслідування шахрайства, учиненого з використанням ЕОТ, що визначає актуальність вказаних методичних рекомендацій.

[1]Української міжбанківської асоціація членів платіжних систем ЄМА. Офіц. Вебсайт: URL :https://www.ema.com.ua/

[2] Кіберполіція України. Офіц. Вебсайт: URL/ https://cyberpolice.gov.ua/news/u--roczi-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-shaxrajstva-v-interneti-8412/

РОЗДІЛ 1
КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА ШАХРАЙСТВ, УЧИНЕНИХ ІЗ ВИКОРИСТАННЯМ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

1.1. Предмет злочинного посягання та способи шахрайств, учинених з використанням електронно-обчислювальної техніки

Аналіз Постанови ПВСУ від 6 листопада 2009 року № 10 «Про судову практику у справах про злочини проти власності» дозволяє нам стверджувати, що предметом шахрайства є майно, яке має певну вартість і, як вже зазначалось вище, є чужим для винної особи: речі (рухомі й нерухомі), грошові кошти, цінні метали, цінні папери тощо.

Стаття 177 Цивільного кодексу України під об'єктами цивільних прав розуміє речі, у тому числі гроші та цінні папери, інше майно, майнові права, результати робіт, послуги, результати інтелектуальної, творчої діяльності, інформація, а також інші матеріальні і нематеріальні блага.

До предмету шахрайства відносить рухоме майно:

а) коштовні речі різного призначення – автомобілі, коштовності, відео- та аудіотехніка і т. ін., гроші, в тому числі у валюті, цінні папери, кольорові метали;

б) гроші, вилучені з обігу, але які підлягають обміну та знаходяться в обігу в банківській чи іншій системі;

в) гроші, давно вилучені з обігу, але які представляють яку-небудь цінність і певну вартість, наприклад, зроблені з дорогоцінних металів, що представляють історичну цінність – рідкі або дуже старовинні й т. ін.

г) безготівкові гроші, що зберігаються на рахунках у банках і кредитних організаціях; д) цінні папери, зокрема, іменні.

д) проїзні квитки на транспорт і транспортні абонементи, за винятком іменних квитків і бланків квитків, що вимагають додаткового оформлення;

е) квитки та абонементи на відвідування театральних спектаклів, концертів, кіносеансів, циркових та інших вистав, виставок і т. ін.; в

ж) квитки різних лотерей (грошово-речових лотерей та ін.);

з) знаки поштової оплати (конверти, марки, листівки тощо);

Під нерухомим майном необхідно розуміти:

а) земельні ділянки, ділянки надр, відособлені водні об'єкти та все, що міцно пов'язане із землею, тобто об'єкти, переміщення яких без збитку, нерозмірного їх призначенню, неможливе, у тому числі ліс, багаторічні насадження, будинки, споруди;

б) предмети державної реєстрації, повітряні й морські судна, судна внутрішнього плавання, космічні об'єкти;

в) надра в межах території України, включаючи підземний простір і корисні копалини, що перебувають у надрах, енергетичні та інші ресурси.

Розкрадання подібнихоб'єктів нерухомості, таким чином, можливо не на рівні розкрадання майна, а тільки на рівні розкрадання прав на нього. Про

розкрадання може свідчити лише офіційний переказ права на нерухомості на ім’я винного або осіб, яких він вкаже.

До предмету посягання шахрайства учинених з використанням ЕОТ,також відноситься інформація, яку можна поділити на:

а) особисту конфіденційну інформацію, якою може бути таємниця листування, телефонних розмов, поштових, телеграфних чи іншої кореспонденції, що передаються засобами зв’язку або через комп’ютер; таємниця всиновлення; особисте життя особи та його таємниця; інформація, яка є об’єктом авторських та суміжних прав; персональні дані, тобто інформація, яка безпосередньо порушує права та свободи громадян; адвокатська таємниця; лікарська (медична) таємниця; таємниця страхування;

б) конфіденційна інформація юридичних осіб: службова таємниця; комерційна або банківська таємниця; редакційна і журналістська таємниця;

в) державна конфіденційна інформація, тобто інформація, яка належить державі чи його суб’єктам: службова таємниця; дані досудового слідства; відомості про заходи безпеки, що застосовуються по відношенню до посадової особи правоохоронних органів або контролюючого органу.

д) інша категорія інформаційних ресурсів – інформація загального користування для необмеженого кола осіб тощо.

В останні часи збільшились випадки заволодінням інформацією про власників платіжних банківських карток та їх реквізити. До такої інформації, як правило, належить: а) ім'я та прізвище держателя картки; б) назва/ код структурного підрозділу банку, що випустив картку; в) термін дії картки; г) номер картки.

При цьому необхідно констатувати, що учинення шахрайства з використанням ЕОТ посягання здійснюється не на нормальне функціонування електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, а на суспільні відносини власності з приводу майна, грошей та інших цінностей, з метою заволодіння якими вчинюється шахрайство. Предметом розглядуваного шахрайства не можуть бути електронно-обчислювальні машини (комп’ютери), системи та комп’ютерні мережі і мережі електрозв’язку. Щодо суб’єктів цих відносин, то подібне шахрайство може бути вчинено будь-якими особами, що використовують електронно-обчислювальні машини (комп’ютери), системи та комп’ютерні мережі та мережі електрозв’язку у власних інтересах, а також особами, які надають відповідні послуги у цій сфері. При цьому, вчиняючи шахрайство, ці суб’єкти здійснюють цілком законні операції з ЕОТ, не порушуючи нормального функціонування електронно-обчислювальних машин.

У сучасному світі, пов’язаному з бурхливим розвитком науково-технічного прогресу, шахрайство набуває все більшого поширення, при цьому впливає майже на всі сфери суспільного життя. У зв’язку із недостатнім науковим дослідженням сучасних способів шахрайств, учинених шляхом незаконних операцій з використанням ЕОТ, виникає багато труднощів як у правоохоронних органів, так і

судів у процесі розкриття, розслідування та правильної правової кваліфікації цих діянь.

У криміналістичній науці вважається загальноприйнятим той факт, що спосіб вчинення кримінального правопорушення є основоположним та системоутворюючим елементом криміналістичної характеристики, що характеризує будь-який злочин, в тому числі і шахрайство, вчинене шляхом незаконних операцій з використанням ЕОТ. При володінні інформацією про спосіб вчинення кримінального правопорушення з'являється можливість висувати обґрунтовані версії про зміст інших елементів криміналістичної характеристики конкретного кримінального правопорушення. Спосіб кримінального правопорушення сприяє встановленню зв'язку злочинця з ознаками інших елементів, він має комплексну структуру, в якій, поряд з правовими елементами характеристики діяння (дії, бездіяльності, провини) злочинця, велике місце належить аналізу процесуальних форм доказування і методики збирання інформації криміналістичними засобами стосовно тієї чи іншої групи кримінальних правопорушень. Встановивши спосіб кримінального правопорушення, слідчий може визначити особу, яка його вчинила. Дуже рідко вдається розкрити кримінальне правопорушення, якщо невідомий спосіб його вчинення, а його встановлення є ключем до виявлення доказів, характерних саме для даного способу. Виявлення способу кримінального правопорушення допомагає розкривати причини і умови, що сприяють його вчиненню.

Це положення відносяться і до способу шахрайств, учинених із використанням ЕОТ, що викликає необхідність звернути на це питання особливу увагу як в теоретичному, так і в практичному плані.

Не дивлячись на те, що проведені ними дослідження є вагомим внеском у вивченні особливостей способу вчинення даного кримінального правопорушення та сприяють його розслідуванню, проблема способу вчинення кримінального правопорушення як одна з ключових у кримінальному праві і криміналістиці залишається як і раніше дискусійною, при цьому в практичній діяльності слідчих НП виникають проблеми в розкритті, розслідуванні та правильній кваліфікації, що потребує більш глибокого та комплексного наукового дослідження способів учинення шахрайств шляхом незаконних операцій з використанням ЕОТ. Це зумовлено, насамперед, розходженням об'єктів дослідження та завдань, на вирішення яких вони спрямовані. Для криміналістики на перший план виступають ознаки способу вчинення кримінального правопорушення, які відображаються у комплексі різноманітних матеріальних та ідеальних слідів, що дозволяє зорієнтуватися у вчиненому діянні та намітити найбільш оптимальні методи його розслідування.

У криміналістичній теорії представлено різні погляди стосовно визначення способу вчинення кримінального правопорушення. Способи шахрайств, учинених з використанням ЕОТ, диференціюються на три основні групи:

1) способи незаконного доступу до банківських рахунків, пов'язані з використанням розрахунків платіжними дорученнями;

2) способи вчинення кримінальних правопорушень, пов'язаних із незаконним доступом до банківських рахунків, пов'язані з використанням операцій у сфері обігу банківських платіжних карток;

3) способи вчинення кримінальних правопорушень, пов'язані з використанням інших засобів доступу до банківських рахунків. Йдеться, наприклад, про: внесення неправдивих відомостей до автоматизованої системи банківської установи; розміщення фіктивного повідомлення на електронній дошці оголошень або Інтернет-аукціоні; несанкціоноване втручання в роботу бортового комп'ютера транспортного засобу з метою ввести в оману щодо показників.

Різновидом шахрайського обману судова практика визнає фіктивне представництво, за якого винний, створюючи враження про свою належність до того чи іншого підприємства, має на меті укласти договори й отримати гроші без поставки товару або, навпаки, одержати товар без належної його оплати. До найбільш поширених випадків застосування обману як способу шахрайства належать: учинення різних угод щодо рухомого і нерухомого майна (купівля-продаж, оренда), коли потерпілому передається фальсифікований товар або предмети гіршої якості, або ж предметом угоди виступають фіктивні предмети, які не існують в об'єктивній реальності або не належать винній особі; незаконне отримання пенсій, субсидій, інших видів соціальної допомоги на підставі підроблених документів: обманне отримання попередньої оплати (авансу) за надання товарів чи послуг.

Обман може мати місце щодо предмета (його ціни, якості, кількості і т. п.), особи (її службового або громадського стану, професії) тощо. Зловживання довірою під час шахрайства є своєрідною формою обману, що полягає в недобросовісному використанні злочинцем певних відносин, які вже склалися між ним і потерпілим. Така форма обману може виникнути тоді, коли між потерпілим і винною особою вже існують відносини, які і породжують певну, можливо тільки зовнішню, довіру між ними. У зв'язку з цим потерпілий передає майно винній особі на підставі довіри до неї та помилкової впевненості у правильності її дій.

Як показує аналіз слідчої та судової практики, для шахрайств, учинених шляхом незаконних операцій з використанням ЕОТ, більш характерна така форма вчинення, як заволодіння грошовими коштами.

Зупинимось на найбільш поширеніших в України.

Фішинг (англ. Phishing) – один з методів шахрайства з використанням соціальної інженерії, який полягає в тому, що зловмисники, імітуючи діяльність реально існуючих компаній або банків-емітентів, використовуючи неголосові засоби комунікації, під різними приводами виманюють у власників платіжних карток реквізити та іншу конфіденційну інформацію. Різновидами фішингу є: 1) фішингові сайти; 2) фішингові електронні листи; 3) фішингові SMS-повідомлення. Крадіжка персональних даних користувача кредитної картки та даних про саму кредитну картку. Метою злочинців у даному випадку є особисті дані, такі як імена, адреси електронної пошти користувача кредитної картки, а також дані кредитних карт або інформація про акаунт (рахунку). У подальшому це дозволяє злочинцям, наприклад, здійснювати замовлення товарів в Інтернеті

під чужим ім'ям і оплачувати їх, використовуючи чужу кредитну карту або списання коштів з чужого рахунку.

Для прикладу. «16.12.2014 року ОСОБА_2, маючи злочинний умисел на заволодіння грошовими коштами держателів платіжних карт шляхом несанкціонованого їх списання через системи on-line платежів. Розуміючи, що для досягнення свого злочинного умислу йому потрібні спільники на роль яких підшукав ОСОБА_3 та ОСОБА_1, який в свою чергу до даної протиправної діяльності залучив ОСОБА_4. В результаті, будучи об`єднаними єдиним умислом, між ними були розподілені злочинні функції наступним чином: собі ОСОБА_2 відвів роль здійснювати телефонні дзвінки потенційним потерпілим та в шахрайський спосіб довідуватись в них реквізити банківських карток відкритих на їх ім`я; ОСОБА_1 доручено підшукати особу, яка б мала доступ до мережі Інтернет та могла здійснити операції по переказу коштів в системі on-line платежів iPay.ua. В свою чергу ОСОБА_1, через ОСОБА_5, ІНФОРМАЦІЯ_2 підшукав ОСОБА_6, ІНФОРМАЦІЯ_3, якого не ставив до відома про дійсність своїх злочинних намірів. Переведення грошових коштів здобутих злочинним шляхом у готівку відводилось ОСОБА_3 та ОСОБА_4 , які відповідно вказівкам ОСОБА_2 та ОСОБА_1, повинні будуть здійснити відповідні операції з зазначеними коштами.

Так, діючи у відповідності до узгодженої всіма учасниками злочинної змови плану 16.12.2014 року о 8 год. 50 хв. ОСОБА_2 зателефонував на мобільний телефон НОМЕР_1, що належить потерпілому ОСОБА_7 та представившись працівником служби безпеки ПАТ КБ «ПриватБанк», тим самим повідомив неправдиву інформацію, яку потерпілий сприйняв за дійсну. В подальшому ОСОБА_2 зловживаючи довірою потерпілого ОСОБА_7 отримав відомості, щодо реквізитів банківської картки ПАТ КБ «ПриватБанк» № НОМЕР_2, а саме строку дії карти, CVV код, після цього, вказані реквізити повідомив ОСОБА_8, а той в свою чергу став консультувати ОСОБА_6 , який в цей час знаходився за місцем свого проживання за адресою АДРЕСА_2 та користувався комп`ютерною технікою підключеною до мережі Інтернет (провайдер ТОВ «Воля-Кабель»). Останній чітко діючи за вказівкою ОСОБА_8 здійснив доступ до web-ресурсу iPay.ua, де заповнив поля для проведення транзакцій реквізитами вказаними йому ОСОБА_8. В результаті чого, на номер мобільного телефону ОСОБА_7 з банківського номеру НОМЕР_3 надійшли «смс» повідомлення з восьмизначними одноразовими паролями. Будучи введеним в оману ОСОБА_7 продиктував їх ОСОБА_2, а він в свою чергу ОСОБА_8, той відповідно ОСОБА_6. Останній не будучи обізнаним про факт неправомірного зняття коштів фактично здійснив транзакції про їх списання з карткового рахунку потерпілого ПАТ КБ «ПриватБанк» № НОМЕР_2 на картковий рахунок № НОМЕР_4 ОСОБА_3, ІНФОРМАЦІЯ_4, здійснивши дві операції: о 9 год. 11 хв. на суму 2905 грн. та о 9 год. 15 хв. на суму 2905 грн. Також, на картковий рахунок № НОМЕР_5 ОСОБА_4, здійснивши дві операції: о 9 год. 26 хв. на суму 2905 грн. та 9 год. 29 хв. на суму 1205 грн. Також, одна операція по поповненню мобільного номеру НОМЕР_6 на суму 298 грн. 08 коп. В подальшому вказані грошові кошти було

знято готівкою ОСОБА_3 в банкоматі за адресою АДРЕСА_3 та ОСОБА_4 в банкоматі за адресою АДРЕСА_4, якими вони розпорядились відповідно до вказівок ОСОБА_2 та ОСОБА_1, а також на власний розсуд. ОСОБА_4, ОСОБА_3, ОСОБА_2, ОСОБА_1 завдали своїми умисними протиправними діями потерпілому ОСОБА_7, матеріальної шкоди на загальну суму 10 218 грн. 08 коп.».

Створення Інтернет-аукціонів шляхом надання недостовірних даних та пропозиції продажу неіснуючих товарів. Зазвичай злочинці реєструються на веб-сайтах Інтернет-аукціонів, частіше всього на «Aukro.ua», «Емаркет Україна» (olx.ua). При цьому шахраї використовують анкетні дані близьких або сторонніх осіб. Після чого на сайті, під своїм доменним іменем, розміщують лот, до якого завантажують фото товару з максимальною вартістю та початковою ставкою, де учасники Інтернет-аукціону, потенційні жертви, дистанційно ставлять ставки на сайті вказаного товару. По завершенню торгів, шахрай зв'язується із жертвою на сайті Інтернет-аукціону, однак часто спілкування може здійснюватись шляхом листування електронною поштою або мобільним зв'язком. Після домовленості в ціні, шахрай надає жертві реквізити банківського рахунку для оплати товару та послуг пересилання, однак, в кінцевому результаті, після перерахування коштів жертва товару не отримує. Шахрай, з метою приховання процесу злочинних дій та самовикриття, може використовувати банківські картки інших осіб та в подальшому переводить в готівку шляхом зняття коштів із банкомату. Більш досвідченіші злочинці, з метою приховання свого місця знаходження, постійно змінюють IP-адреси, що створює труднощі у встановленні місця знаходження шахрая.

Отримання данні про банківську картку та подальше перерахування коштів із банківських карток потерпілого. Для вчинення вказаного виду шахрайства, шляхом незаконних операцій з використанням ЕОТ, злочинці на сайтах Інтернет-торгівлі підшукують жертв. Знайшовши інформацію потенційної жертви про продаж товарів, шахраї встановлюють з останньою контакт. Під час розмови з жертвою шахраї неправдиво повідомляють, що будуть здійснювати купівлю товарів, та для перерахунку грошових коштів за покупку дізнаються номер її банківського карткового рахунку. Після чого шахрай телефонує жертві та представившись працівником банку повідомляє інформацію про неможливість перерахунку коштів на карту потерпілої. Після чого, в ході телефонної розмови, неправдиво повідомляють, що для зарахування грошових коштів їй необхідно повідомити конфіденційні дані банківської картки (анкетні дані жертви, захисний код картки та дівоче прізвище матері), або підійти до терміналу банкомата та виконати необхідні операції для нібито зарахування коштів на її банківську картку. Під час розмови по телефону з жертвою, шахрай диктує відповідні комбінації, які остання виконує, та шляхом обману і незаконних операцій з використанням електронно-обчислювальної техніки отримує грошові кошти.

У подальшому шахрай, використовуючи електронні платіжні системи мережі Інтернет («Портмоне», ГлобалМані, EasyPay, LiqPay, iPay.ua, Простір), перераховує грошові кошти з карткового рахунку потерпілої на свій банківський рахунок або рахунок третіх осіб, яким навіть не відомо, що з їх банківськими

картками проводяться злочинні операції. Для того, щоб жертва відразу не дізналась, що відносно неї вчинено шахрайство, злочинці надсилають на мобільний номер останньої SMS-повідомлення про зарахування коштів на банківську картку.

Обманне заволодіння грошовими коштами шляхом створення або використання сайтів благодійних організацій. При використанні благодійних сайтів, злочинці надсилають листи від імені благодійних організацій або людей, яким потрібна допомога. При цьому посилання можуть належать реальним благодійним фондам, але реквізити для перерахування коштів належать шахраям.

Крім цього, злочинці шляхом незаконних операцій з використанням ЕОТ, створюють сайти благодійних організацій, на яких публікують оголошення з проханням про матеріальну допомогу на лікування хворим дітям. Також шахраї на вказаних сайтах можуть розміщувати вигадану інформацію стосовно хвороби, при цьому розміщують чужі фотографії людей, які потребують фінансової допомоги на лікування, або копіюють оголошення із сайтів благодійної допомоги, які належать реальним людям, змінюючи реквізити для перерахування грошей.

Заволодіння майном шляхом створення і забезпечення діяльності Інтернет-магазину. Під час створення сайту Інтернет-магазину шахрай може діяти як самостійно, так і у складі злочинної групи. Це більш складний спосіб, ніж продаж товарів на Інтернет-аукціоні, і складається з декількох етапів. Спочатку шахраї створюють у мережі Інтернет сайти у вигляді Інтернет-магазинів – аналогів Інтернет сайтів, що діяли на території України чи інших держав, та які б функціонували на території України. На вказаних сайтах розміщують завідомо неправдиву інформацію у вигляді оголошень щодо продажу товарів, яких в наявності ніколи не було. Наступним етапом є створення та отримання контролю над фіктивними підприємствами, відкриття банківських рахунків, на які замовники/клієнти фіктивних Інтернет-магазинів в подальшому здійснюють передоплату у вигляді грошового переказу за придбання замовленого товару за реквізитами належних їм пластикових карток, відкритих в банках України. При цьому назви фіктивних підприємств повинні бути подібними до назв фіктивних Інтернет-магазинів, щоб викликати довіру у користувачів.

Після чого здійснюється оформлення договорів з операторами телефонного зв’язку про надання послуг зв'язку та Інтернет-зв’язку, так званої «SIP-телефонії», телефонні номери яких слугують для зворотного зв’язку з замовниками Інтернет-магазинів. При цьому у вхідних дзвінках на телефони замовників фіктивних Інтернет-магазинів відображаються міські номери телефонів, що викликає довіру в користувачів.

Для прикладу. «*У невстановлений слідством день та час, в період з червня по серпень 2016 року ОСОБА_1, маючи навички роботи із комп`ютерною технікою та інтернет ресурсами, з використанням електронно-обчислювальної техніки персонального комп’ютера, знаходячись в м. Житомирі, використовуючи свій обліковий запис, зареєстрований на сайті Інтернет оголошень «http://kloomba.com», «https://ukrrover.jimdo.com», «http://klubok.com», та сайті Інтернет оголошень «http://OLX.ua», з метою подальшого незаконного*

заволодіння коштами потенційних клієнтів шляхом обману, розмістив на вказаних сайтах оголошення на продаж різноманітних товарів, які насправді не мав наміру продавати, в результаті чого вчинив ряд умисних, корисливих кримінальних правопорушень за наступних обставин.

27.06.2016 року ОСОБА_2 (м. Буча Київської області) у всесвітній мережі загального доступу «Інтернет» переглядала сайт оголошень «http://OLX.ua» та побачила оголошення про продаж дитячого біговела вартістю 700 грн. 00 коп., яке розмістив користувач вище вказаного сайту, при цьому зазначив свій контактний номер мобільного телефону НОМЕР_1. Після цього, ОСОБА_2, будучи введеною в оману користувачем номеру мобільного телефону НОМЕР_1 , який належить ОСОБА_1, домовилася про купівлю вказаного товару, при цьому ОСОБА_1, маючи умисел, спрямований на заволодіння чужим майном шляхом обману, повідомив ОСОБА_2, що умовою передачі товару є лише 100-відсоткова оплата його вартості.

На виконання вказаних домовленостей ОСОБА_2 27.06.2016 року, будучи неправдиво запевненою в добросовісності намірів ОСОБА_1, здійснила перерахування готівкових коштів в сумі 700 грн. 00 коп., на банківський картковий рахунок № НОМЕР_2, відкритий у ПАТ КБ «УкрСиббанк» на ім`я ОСОБА_1. При цьому, ОСОБА_1 завірив ОСОБА_2 , що після перерахування грошових коштів за замовлений товар, одразу надішле на ім`я останньої оплачений товар.

Після цього, ОСОБА_1, отримавши грошові кошти в сумі 700 грн. 00 коп., порушуючи попередню домовленість, вказаний товар не надіслав, отриманими грошовими коштами розпорядився на власний розсуд.

Таким чином, ОСОБА_1 незаконно, шляхом обману (шахрайство), та незаконних операцій з використанням електронно-обчислювальної техніки, заволодів грошовими коштами ОСОБА_2 в сумі 700 грн. 00 коп., чим спричинив останній матеріальної шкоди на вказану суму.».

В окремих випадках вчиняються дії зі створення, організації та забезпечення діяльності структурної частини злочинної групи, а саме «кол-центру», оператори якого спілкуються з клієнтами, імітуючи діяльність кол-центрів справжніх Інтернет-магазинів, приймають замовлення та надають реквізити для перерахування грошових коштів. Крім цього, шахраї розроблюють спеціальну web-сторінку з базою даних для роботи організаторів та операторів «кол-центру», за допомогою якої злочинці приймають та ведуть облік замовлень. Після вчинення шахрайських дій, так звані оператори «кол-центру» заносять телефонні номери ошуканих клієнтів до «чорного списку», щоб вони не заважали роботі «кол-центру» та якнайдовше не здогадувались, що відносно них було скоєно шахрайство.

Створення та діяльність фіктивних фінансових бірж. Діяльність таких бірж забезпечується діяльністю злочинної групи, яка складається та маскується за офіційно зареєстрованими підприємствами. Зловмисники використовують методи агітаційного характеру для залучення громадян до інвестування коштів у торгівлю на фінансових ринках. Шахраї пропонують потенційним клієнтам купувати цінні

папери для отримання прибутку. Використовуючи бренди «hqbroker» та «trade12», злочинці задіюють різні веб-ресурси для імітації добросовісної ділової репутації. Після чого так звані «брокери» створюють у потерпілого помилкову уяву про процес здійснення торгів на світових біржах. Для цього вони використовують вже встановлене на комп'ютер потерпілого спеціальне програмне забезпечення для проведення торгів, яке фактично надає можливість здійснювати віддалений контроль за його комп'ютером. Такі компанії створюють уяву у потерпілих про співпрацю з іноземними компаніями, які торгують цінними паперами, які є учасниками фондового ринку та мають відповідні дозволи та ліцензії на здійснення зазначеної діяльності у світі. Такими діями злочинці спонукають потерпілого вносити свої кошти на рахунок шахрайського торгівельно-сервісного підприємства, переслідуючи при цьому мету – заволодіння його коштами під приводом укладання угод з купівлі-продажу цінних паперів.

Крім цього, аналогічним способом, учасники групи організовують діяльність офісів для «операторів», «технічних працівників» та «брокерів». Такі офіси можуть розміщувати у різних містах. Свою діяльність шахраї «прикривають» офшорною компанією. Для вчинення протиправної діяльності злочинці використовують спеціально створений для цього он-лайн ресурс (Інтернет-майданчик), де нібито відбувалися успішні он-лайн торги валютними парами (бінарні опціони). За схемою, потенціальному клієнту пропонують прийняти участь в торгах, шляхом відкриття спеціального демо-рахунку, де організаторами створюється імітація успішних торгів. Після чого, особу шляхом обману скеровують на відкриття реального рахунку. При цьому, з потерпілими працюють «оператори» офісу, які націлюють їх на внесення якомога більших внесків. Аргументують це більшою вірогідністю виграшу. Для досягнення цієї мети зловмисники використовують заздалегідь прописану схему психологічного впливу на жертву. Вклавши гроші, потерпілі не мають можливості їх «зняти». В даному випадку вони можуть лише поповнювати рахунки. Система працює таким чином, що всі торги призводять до повної втрати грошей користувачів.

Також у 2020 році набули популярності шахрайські схеми, замасковані під сервіси доставки платформ оголошень. У такому випадку злочинці розміщували оголошення про продаж товарів і для обговорення деталей пропонували перейти у месенджери. Туди покупцям надсилали фальшиві накладні для сплати або посилання на фейковий ресурс, де потрібно оформити доставку. Однак врешті оплата надходила не на платформу оголошень, а на картку шахрая.

Аналіз визначених вище та інших способів шахрайства, учинених з використанням ЕОТ, дозволяє їх поділити за наступними критеріями.

1. Залежно від періодичності вчинення кримінального правопорушення:

1) одноразові (шахрайство вчиняється з метою обману однієї визначеної особи з метою заволодіння певним товаром, що належить їй, або сумою грошей за продаж неіснуючого товару). Наприклад заволодіння коштами шляхом імітування продажу неіснуючого товару шляхом розміщення відповідних повідомлень на сайті OLX.ua;

2) тривалі (шахрайство вчиняється з метою обману невизначеного кола осіб). Наприклад, шляхом створення сайту з продажу послуг (туристичних) чи товару (медичних масок) невизначеної кількості осіб.

2. Залежно від сфери застосування:

1) банківська (виманювання або інше незаконне отримання конфіденційних даних клієнта банку та подальше перерахування коштів з банківських рахунків та отримання додаткових кредитів);

2) побутова (отримання речей, що дорого коштують, за документами своїх родичів, за викраденими чи знайденими документами);

3) страхування (надання не існуючих страхових полісів);

4) туристична галузь (надання не існуючих туристичних послуг);

3. В залежності від кількості задіяних до вчинення шахрайства осіб:

1) вчинено за участю однієї особи;

2) вчинено групою осіб;

3) вчинено організованою групою осіб;

4. Залежно від предмета посягання:

1) грошові кошти;

2) матеріальні цінності:

– побутові предмети;

– рухоме майно, зокрема транспортні засоби;

4) інформація про особистість, акаунт або банківську картку;

5) право на майно, зокрема на нерухоме.

5. Від виду ЕОТ, яка використовувалась:

1) комп'ютери та ноутбуки;

2) телефони;

3) планшети;

4) інші види.

6. В залежності від інформаційної підтримки:

1). цілеспрямоване створення окремого Інтернет-сайту;

2) розміщення інформації на вже існуючих Інтернет-сайтах;

3) шляхом несанкціонованого доступу до ЕОМ потерпілого;

7. Залежно від характеру «стосунків», що виникають між потерпілим та злочинцем:

1) установчі дані злочинця не відомі;

2) попередні дані про особу-злочинця відомі;

3) відомі попередні дані лише про одну особу, яка дія у складі групи осіб.

8. Залежно від місця створення та місця реєстрації IP-адреси ЕОТ:

1) місце знаходження встановлено (Україна);

2) місце знаходження – за кордоном (країна та установчі дані провайдера відомі);

3) місце знаходження – тимчасово окуповані території Донецької та Луганської областей або окупованій та у подальшому анексованій Автономній Республіки Крим;

4) місце знаходження країни – не встановлено.

9. Залежно від способів введення в оману або зловживання довірою:

1) маніпулювання якістю інформації, тобто фальшування деяких фактів або навмисне укривання істини;

2) маніпулювання кількістю інформації, тобто укриття частини правди або паралельне подання не існуючих та існуючих фактів як істини;

3) повідомлення двозначної або неконкретизованої інформації;

4) умовчування – повне приховування правди;

5) спотворення – навмисне повідомлення помилкової інформації.

10. За характером подання відомостей:

1) активний (повідомлення потерпілому неправдивих відомостей про певні факти, обставини, події);

2) пасивний (умисне замовчування юридичне значимої інформації) характер.

11. За новизною способу вчинення шахрайства:

1). Спосіб обману (зловживання довірою) не відомий в правоохоронній практиці;

2) Спосіб обману (зловживання довірою) зустрічався раніше в правоохоронній практиці;

12. За ступеню доведеності кримінального правопорушення:

1) шахрайство частково реалізоване;

2) шахрайство реалізоване;

3) шахрайство припинене.

13. В залежності від способу підготовки до вчинення шахрайства:

1) вчиненню шахрайства сприяв несанкціонований доступ до ЕОТ;

2) вчинення шахрайства здійснювалось з використанням шкідливих програмних чи технічних засобів;

3) вчиненню шахрайства сприяло розповсюдження рекламної чи іншої продукції про предмет посягання (надання послуг).

1.2. Слідова картина та обстановка шахрайств, учинених з використанням електронно-обчислювальної техніки

«Слідова картина» є обов'язковим елементом криміналістичної характеристики кримінальних правопорушень, оскільки її зміст виступає практичним інструментом і своєрідним орієнтиром у виборі напрямів їх розслідування.

Залежно від обставин та способів шахрайства, учиненого з використанням ЕОТ, про вчинення вказаного кримінального правопорушення може свідчити наступна слідові картина на місці подіїя, яких може бути декілька:

– місце події потерпілого від вчинення шахрайства;

– місце події, з якого вчинялося шахрайство, з використанням ЕОТ.

Слідові картина на місці події, яким як правило є місце проживання чи роботи потерпілого, від вчинення шахрайства, характеризується наступними

слідами, а саме наявність ЕОТ (комп'ютери, їх системні блоки, ноутбуки), якими користувався потерпілий під час вчинення шахрайства щодо нього, у якому містяться цифрові сліди, які залишилися внаслідок вчинення такого кримінального правопорушення.

Що стосується місце події, з якого вчинялося шахрайство, з використанням ЕОТ, то в даному випадку йому характерна наявність наступних предметів, де можуть знаходитись сліди кримінального правопорушення:

– ЕОТ (комп'ютери, їх системні блоки, ноутбуки);

– периферійні пристрої (монітори, принтери, дисководи, модеми, сканери, клавіатури, маніпулятори, джойстики та інше), комунікаційні прилади комп'ютерів і обчислювальних мереж;

– носії інформації (жорсткі диски, флопі-диски, оптичні диски, флеш-пам'ять, зовнішні HDD);

– засоби зв'язку (у разі їх використання під час вчинення шахрайства) (на стільникових апаратах, засобах телекомунікації, спеціальних електронних картках, електронних ключах доступу до персонального комп'ютера; пристроях упізнання користувача);

– електронні записні книжки, інші електронні носії текстової або цифрової інформації, технічна документація до них;

– предмети, отримані в результаті вчинення кримінального правопорушення (речі, гроші, інше майно);

– сліди пальців рук та мікрочастинки або мікрооб'єкти (наприклад, частки волосся), які можуть залишатися на вказаних вище предметах;

– сліди, що залишаються на «робочому» місці злочинця, (наприклад, які-небудь рукописні записи – списки паролів, коди, чернетки тощо).

Також цифрові сліди можуть утворюватись за результатами спілкування жертви зі злочинцем у вигляді бази даних абонентів операторів зв'язку. Зокрема, важливу криміналістично-значущу інформацію можна отримати при вивченні даних електронного листування та сервісів обміну SMS (Short Messaging Service – служба коротких повідомлень). В атрибутах файлів електронних листів міститься дата й час відправлення, електронна адреса відправника, найменування й адреса інтернет-провайдера та інша інформація. Найменування й адресу інтернет-провайдера, за допомогою якого злочинець, підключений до мережі Інтернет, може вільно отримати через спеціальну службу Whois (у мережі Інтернет), зазначивши IP-адресу «атакуючого» комп'ютера. Телефонні дзвінки з мобільного телефону та тексти SMS-повідомлень автоматично фіксуються й накопичуються на сервері оператора мобільного зв'язку та можуть бути отримані слідчим.

Що стосується цифрових слідів – це сліди у свідомості людини, що являють собою специфічну форму вищого рівня психічного, цілеспрямованого, активного, вибіркового відображення, здійснюваного в чуттєво-раціональній формі, в результаті якого формується відносно адекватний, суб'єктивно-об'єктивний «відбиток» – уявний образ у пам'яті людини, заснований на раніше сприйнятій інформації та є формою збереження відповідної інформації.

Питанням дослідження проблем боротьби зі злочинами, які вчиняються з використанням цифрових пристроїв, учені-криміналісти приділяють значну увагу. Науковці зазначають, що традиційний розподіл слідів у криміналістиці на сліди в широкому сенсі (результат будь-якої матеріальної зміни первинної обстановки внаслідок учинення кримінального правопорушення) та у вузькому (відображення під час учинення кримінального правопорушення на одному з об'єктів взаємодії слідів зовнішньої будови іншого об'єкта) практично не охоплює злочини, що вчиняються з використанням цифрових засобів. В окремих працях зазначено, що на сучасному етапі розвитку криміналістики як сліди розглядаються й електронні (цифрові).

За результатами вчинення шахрайств з використанням ЕОТ, залишаються як матеріальні, так і цифрові сліди. Цифрові сліди цих кримінальних правопорушень отримуються під час проведення слідчих (розшукових) та інших процесуальних дій у більшості випадків з пам'яті ЕОТ, а також свідків чи осіб, які вчинили це кримінальне правопорушення чи причетні до його вчинення.

Цифровий слід має певну систему ознак у вигляді окремих інформаційних елементів, які можуть бути записані як на одному, так і на декількох носіях цифрової інформації. Носії таких слідів можуть бути одночасно підключені до декількох цифрових пристроїв, об'єднаних, наприклад, у телекомунікаційну мережу.

Час роботи користувача в мережі Інтернет на певній ЕОТ можна встановити за спеціальним log-файлом (журналом), додаткові відомості про вид, порядок і час підключень користувача до мережі і збіг цих даних з log-файлом провайдера може слугувати вагомим доказом викорситання саме цієї ЕОТ для вчинення шахрайства.

З тим, що не існує проблем встановлення часу вчинення кримінальних правопорушень з використанням ЕОТ не складає великих проблем, оскільки операційна система електронного пристрою детально стежить практично за кожною важливою операцією, інформація про які відображається в статистичних файлах. За допомогою програм загальносистемного призначення можна встановити поточний час роботи комп'ютерної системи. Це дозволить за відповідною командою вивести на екран дисплею інформацію про день, години, хвилини та секунди виконання тієї або іншої операції.

На сайтах соціальних мереж (наприклад, Facebook, Twitter, LinkedIn, Instagram та ін.) можна виявити електронні сліди у вигляді повідомлень і коментарів осіб, що перевіряються, їх персональних даних (наприклад, електронну адресу), фотознімків і відеозаписів, історію пошукових запитів та ін. Ці сліди містять інформацію про час відвідування сайту і деякі персональні дані користувача (наприклад, його електронну адресу), за якими можна здійснити пошук його номера телефону, дати народження, місця роботи та проживання, визначити коло спілкування та інтереси.

Так само, на сторінці веб-сайту також можуть міститися віртуальні сліди (фотографії, відгуки та коментарі стосовно певних лотів, результати переписки між користувачами та продавцями тощо). Сліди можуть міститися й у історії

голосових повідомленнях та і відеодзвінках. Втім, найцінніша інформація криється у доменній адресі (IP-адреси), що дозволяє встановити місцезнаходження точки доступу до комп'ютера, з якого здійснювалося спілкування.

Оскільки здебільшого шахраї і потерпілі обирають спосіб електронних розрахунків через електронні платіжні засоби та системи, електронні гаманці, інші види безготівкових розрахунків, у телефоні, в комп'ютері може міститися програмне забезпечення, звідки можна отримати слідову інформацію про проведені банківські операції. За таких обставин банківська карта, рахунок власника картки або рахунок телефонного номера виступають об'єктом слідоутворення.

Також носіями вертуальних слідів шахрайства, учиненого з використанням ЕОТ, є очевидці кримінального правопорушення (наприклад, особи, які були присутні під час створення сайту, аканту злочинця, використання ЕОТ з протиправною метою чи інших незаконних дій з ним), при цьому, вони могли не знати подальшу мету цих дій. Таким чином, про вчинення шахрайства можуть свідчити ідеальні сліди, тобто ті сліди, що залишилися в пам'яті людей, і ми можемо отримати їх шляхом проведення допиту особи (свідків, потерпілих, затриманих).

Особливістю утворення ідеальних слідів є відсутність прямого контакту між взаємодіючими об'єктами. Оскільки ідеальне відображення здійснюється у формі свідомості, то об'єктом, що відображає, є тільки людина як єдиний його носій. При утворенні матеріальних слідів об'єктом, що відображає, може також бути людина, але тільки як тілесна істота.

При допиті, свідок описує не саму подію, а образ дійсності, який зберігся в його пам'яті, що може не збігатися у всіх деталях з реальною подією. Звідси стає зрозумілим, чому свідки, що спостерігали ту саму подію, описують її по-різному, тобто різним є суб'єктивне відображення. Уявна (образна) форма – суб'єктивна форма психічного відображення. Іншими словами, суб'єктивна сутність уявного образу визначається індивідуальністю сприйняття, запам'ятовування й відтворення ідеального відображення.

Ідеальні сліди потребують вжиття відповідних заходів щодо їх перевірки. Так, оцінка слідів пам'яті про спосіб шахрайства, учинене з використанням ЕОТ, проводиться комплексно з урахуванням слідів інших видів взаємодії, що знаходяться відносно досліджуваного моменту часу в синхронічному або поліхронічному зв'язку.

Можна виділити групи осіб, в пам'яті яких залишаються ідеальні сліди шахрайств, учинених з використанням ЕОТ, тобто таких, що залишаються в пам'яті підозрюваних, потерпілих та свідків, то їх можна поділити на групи залежно від осіб, які є їх носіями:

1) сліди, що зберігаються у пам'яті осіб, які безпосередньо сприймали обставини вчинення кримінального правопорушення (потерпілий та його родичі, інші особи, які входять до вузького кола спілкування з потерпілим і знаходяться в довірчих чи дружніх стосунках із злочинцем);

2) сліди, що зберігаються у пам’яті осіб, яким відомі обставини, що передували вчиненню шахрайства;

3) сліди, що зберігаються у пам’яті осіб, які безпосередньо бачили весь процес шахрайства чи його складові, учинені з використанням ЕОТ;

4) сліди, що зберігаються у пам’яті осіб, яким відомий підозрюваний у зв’язку із вчиненням ним шахрайства;

5) сліди, що зберігаються у пам’яті осіб, з якими підозрюваний підтримує дружні чи сімейні стосунки (родичі, сусіди, приятелі), і які мають на меті приховати факт причетності підозрюваного до вчинення кримінального правопорушення.

За наявності ідеальних слідів кримінального правопорушення, вони закріплюються у процесуальних документах (протоколах допиту свідків, підозрюваного, потерпілого), на підставі яких вживаються процесуальні дії, спрямовані на ефективне розслідування шахрайства, учиненого з використанням ЕОТ.

Матеріали слідчо-судової практики свідчать, що типовими місцями вчинення шахрайств, з використанням ЕОТ, є місце проживання злочинця, місце роботи, а також спеціально вибрані місця, де є доступ до мережі Інтернет, зокрема ті місця, де не встановлено відеокамери, які дають змогу зафіксувати перебування у таких місцях злочинця. До таких місць, як правило, належать заклади харчування, де присутня мережа Інтернет, громадські місця, де поширено розповсюдження WI-FI, місця позбавлення волі. Непоодинокі випадки, коли шахрайства, учинені з використанням ЕОТ, можуть вчинятися поза межами нашої держави, а також з тимчасово окупованих районів Донецької та Луганської областей, Автономної Республіки Крим.

Окрім того, з метою приховування IP-адрес злочинці активно використовують спеціальні програми, які не завжди дають змогу правоохоронним органам встановити місце входу ЕОТ в мережу Інтернет.

Так, перевагами VPN-з’єднання є наступні: сервери розташовані в 20 країнах світу; постійно додаються нові сервери; VPN-з’єднання захищає конфіденційність користувача і підвищує рівень безпеки; працює безкоштовно 7 годин на тиждень; забезпечує конфіденційності і захист через VPN; можливість приховати свій IP-адрес; шифрування інтернет-даних; захист персональних інтернет-даних за допомогою надійного 256-бітного шифрування; використання будь-яких потрібний сайтів без будь-яких обмежень; надає можливість видалити банери і системи відстеження.

Windscribe, надає 10 ГБ безкоштовного трафіку в місяць і можливість виходу в Інтернет через 25 серверів в 11 країнах. Для реєстрації не потрібні особисті дані, сервіс запитує лише логін і пароль. При бажанні можна вказати свій email, щоб отримати доступ до акаунту, якщо забудете пароль. На цю ж пошту будуть приходити повідомлення про нарахування нових лімітів трафіку.

Вчиненню шахрайству, з використанням ЕОТ, сприяють головним чином обстановка слабкого контролю за дотриманням встановленого порядку обігу контенту провайдерами, що надають Інтернет послуги, власниками вебсайтів,

інтернет мереж, соціальних мереж, недостатня захищеність комп'ютерних систем. Тут злочинці частіше використовують вже об'єктивно сформовані для них сприятливі умови, чим спеціально створювані ними.

1.3. Особа злочинця та особа потерпілого шахрайств, учинених з використанням електронно-обчислювальної техніки

Особа злочинця є центральним елементом криміналістичної характеристики шахрайств, що вчиняються з використанням ЕОТ, оскільки предмет злочинного посягання, спосіб кримінального правопорушення, його слідова картина завжди пов’язані з особистісними ознаками особи злочинця та закономірностями його поведінки. Дослідження особи злочинця оптимізує процес висунення слідчих версій і забезпечує обрання найбільш оптимальних тактичних прийомів проведення окремих СРД при розслідуванні шахрайств, що вчиняються з використанням ЕОТ. За допомогою аналізу поведінки та психології злочинця можна встановити дійсні причини й умови вчиненого кримінального правопорушення, оцінити суспільну небезпеку злочинця, здійснити правильну кримінально-правову кваліфікацію вчиненого і, як наслідок, призначити справедливе покарання.

Пропонується наступна структуру характеристики особи:

а) соціально-демографічна;

б) морально-психологічна;

в) фізіологічно-розумова характеристика – спрямованість і характер учиненого кримінального правопорушення, наявність досвіду роботи в Інтернет-мережі, учинення кримінального правопорушення в складі групи чи організованої злочинної групи тощо.

При цьому у даному випадку пропонується вивчати таку особу: 1) за залишеними нею слідами за результатами використання ЕОТ та 2) в процесі розслідування кримінального правопорушення в залежності від способу вчинення шахрайства.

Особистими характеристиками портрета такої особи – є активна життєва позиція, нестандартність мислення і поведінки, обережність, уважність. Також зустрічаються серед таких осіб фахівці у сфері психології, економіки, а й інколи і в різних галузях права. Деяким із них добре відомі методи роботи правоохоронних органів.

Однією з характерних особливостей шахрайства, які вчиняються з використанням ЕОТ, зокрема, є відсутність судимості у злочинців. Зазвичай такі шахрайства вчиняються з корисливих мотивів. Хоча, останнім часом широкого розповсюдження набувають шахрайства з використанням ЕОТ особами, які знаходяться в місцях позбавлення волі.

Що стосується психологічних ознак осіб, які вчиняють шахрайство з використанням ЕОМ, то тут необхідно зазначити, що вони досить в психології, володіють різними методами так званого заманювання осіб придбати ту чи іншу

річ, при цьому вони використовують не найкращі людські якості: корисливість, пихатість, сластолюбство. Техніки виконання шахрайських прийомів різноманітні.

Значна кількість шахрайств, що вчиняються з використанням ЕОТ, має специфічну ціннісну орієнтацію шахрая, а саме його відношення до жертви як до неживого об'єкта. Людина для нього насамперед – це можливе джерело власних матеріальних благ. Внутрішній світ жертви, її переживання, страждання у разі позбавлення матеріальних цінностей для злочинця не мають значення.

У шахрайських посяганнях на перший план виступає яскраво виражений корисливий мотив. Проте, окрім користі, мотивами шахрайської діяльності можуть бути: самоствердження, приховане прагнення до влади. Залежно від домінування того або іншого мотиву у разі вчинення кримінального правопорушення кримінального правопорушення пропонується поділити шахраїв, що використовують маніпуляцію свідомістю і поведінкою жертв, на такі групи:

1) шахраї з провідним корисливим мотивом, раціональним підходом до способу вчинення шахрайства, підготовкою до його вчинення і усвідомленням усіх наслідків злочинної діяльності;

2) шахраї з провідним ігровим мотивом (шахрай – гедоніст, що отримує задоволення від процесу злочинної діяльності);

3) шахраї з ведучим ситуативно виниклим мотивом, під впливом сприятливих (з точки зору реалізації злочинного задуму) обставин;

4) шахраї з провідним мотивом, що виник під впливом групового тиску.

Серед шахраїв, які орудують через мережу Інтернет, найбільше зустрічаються злочинці з корисливими та ігровими мотивами. В основі мотивації корисливих злочинців, зокрема шахраїв, лежать гіпертрофовані (завищені) матеріальні потреби. Корисливі злочинці здебільшого не бачать цінностей поза матеріальною сферою, основною їхньою властивістю є неконтрольоване прагнення до матеріального збагачення.

Що стосується фізіологічно-розумової характеристики шахраїв, то в більшості випадків ними є особи, які володіють навичкам використання комп'ютерної техніки та інших електронних засобів, вміння працювати в мережі Інтернет, та в окремих випадках, вузьку спеціалізацію, оскільки виконати певні дії з ЕОТ з метою вчинення шахрайства може обмежене коло осіб: а) аматори, тобто ті, що діють самостійно, в домашніх умовах і вільний від роботи час, б) високоосвічені спеціалісти, які діють у складі організованих злочинних груп. Необхідно підкреслити, що до складу такої групи обов'язково входить один або кілька учасників, які є програмістами або хоча б володіють знаннями та навичками в галузі комп'ютерних інформаційних технологій.

Злочинець особисто не контактує із своєю жертвою, а здійснює свої злочинні дії шляхом телефонних розмов, надсилання SMS-повідомлень або через Інтернет-листування. Типологія особи диференціюється на відмінностях характеру антигромадської її спрямованості та ціннісних орієнтаціях, до яких належить негативне ставлення до важливих благ людської особистості.

Виходячи із загальних положень криміналістичної характеристики, результатів кримінологічних досліджень, необхідно виділити ті властивості особи, яка вчиняє шахрайські дії з використанням ЕОТ, вивчення яких дозволяє розробити рекомендації для обрання правильного напрямку розслідування, забезпечення найбільш ефективної тактичної лінії у провадженні слідчих (розшукових) дій; встановити, які риси цієї особи повинні враховуватися при виявленні цього виду кримінального правопорушення і їхньому розкритті. Особа шахрая, який вчиняє кримінальне правопорушення з використанням ЕОТ, характеризується специфічним комплексом ознак. Більшість злочинців мають сильний дар уяви, вони використовують вплив і вміння переконувати людей.Щодо якостей особистості злочинця, варто встановити те, що в деяких випадках однією з важливих якостей особистості Інтернет-шахрая є наявність організаторських здібностей, оскільки деякі види інтернет-шахрайства є технічно складними в плані виконання, а тому у їх вчиненні можуть брати участь кілька людей.

В залежності від прихильності осіб використовувати певні способи для заволодіння майном шляхом шахрайства, учиненого з використанням ЕОТ, пропонують наступну класифікацію таких осіб.

Кардери. Спеціалізуються на махінаціях з пластиковими картками, оплачуючи свої витрати з чужих кредитних карток. Типова процедура кардинга полягає в копіюванні інформації, що міститься на магнітній смузі кредитної картки (дамп) і виробництві фальшивої картки-«фантома» з нанесенням на неї скопійованого дампа або одержанням індивідуального пін-коду від власника реальної карти, наприклад, методами соціальної інженерії. Ці особи також займаються викраденням номерів кредитних карт з подальшим отриманням доступу до рахунків осіб, чиї номери і коди кат були викрадені. Цією групою використовуються різні методи, від елементарного підглядання коду карти з наступною крадіжкою самої карти до крадіжки номерів з пам’яті ЕОТ, створення підставних банкоматів та Інтернет магазинів.

Кіберкруки. Спеціалізуються на несанкціонованому проникненні в комп’ютерні системи та мережі фінансово-банківських установ і закриті комп’ютерні системи та мережі державних силових структур та органів. Використовують комп’ютерні системи та мережі для викрадення грошових коштів, отримання цінної фінансової інформації. Популярним предметом посягання є кредитна інформація, інформаційні бази даних правоохоронних органів та інших державних і комерційних структур. Тому, нерідко отриману інформацію вони продають іншим особам.

Фішери. Їх метою є заволодіння обманним шляхом персональними даними клієнтів онлайн-аукціонів, інтернет-магазинів, сервісів грошових переказів та іншої конфіденційної інформацією. Постійно удосконалюються шахраями різні «схеми», які спрямовані, в основному, на занадто довірливих або неуважних користувачів, які самі (добровільно) надають конфіденційну інформацію, коли їх просять повторити введення пароля, повідомити номер рахунку та пароль для реєстрації покупки або грошового переказу, зареєструватися на лже-сайті

інтернет-магазину, тощо. Фішери створюють підставні сайти (наприклад копії сторінки банку), заходячи на який власник карти, бажаючи перевірити свій рахунок, вводить конфіденційні дані, які згодом використовуються зловмисником.

Спамери. Займаються масовою (більш ніж 5-ти адресатам) розсилкою (часто анонімних) оголошень засобами електронних комунікацій, насамперед – по електронній пошті чи в соціальних мережах. Як правило, діють в інтересах третіх осіб за матеріальну вигоду.

Кіберсквотери. Це особи що здійснюють захоплення доменних імен з метою наживи. Доменні імена часто називають «нерухомістю» онлайнового століття. Добре підібране ім'я може само по собі забезпечувати досить сильний потік відвідувачів, а значить, і потенційних клієнтів: вдала назва інтуїтивно перебуває й легко запам'ятовується. Усвідомлення цінності доменів постійно зростає, а слідом зростає і їхня ціна.

Фрікери. Спеціалізуються на використанні телефонних систем, зломі цифрових станцій телефонного зв'язку телефонних компаній, несанкціонованому отриманні кодів доступу до платних послуг ISDN, крадіжці і підробці телефонних карток, з метою уникнути оплати за надані телефонні послуг. Їх злочинна діяльність спрямована на отримання кодів доступу, розкрадання телефонних карток і номерів доступу з метою перенести оплату на рахунок іншого абонента.

Поняття *потерпілого* міститься у частині першій ст.49 КПК України: «Потерпілим визнається особа, якій злочином заподіяно моральну, фізичну або майнову шкоду». Особа потерпілого є суттєвим елементом криміналістичної характеристики досліджуваної категорії кримінальних правопорушень. Відомості про особу жертви безпосереднім чином «проливають світло» на інші обставини події кримінального правопорушення.

Зважаючи на специфіку досліджуваного нами виду шахрайства доречно зазначити, що потерпілим може бути будь-яка особа: громадянин України, іноземець чи особа без громадянства, що постійно проживає на території України, та повинен мати повну цивільну дієздатність.

В контексті дослідження особи потерпілого від шахрайства представляється слушним встановлення відношення самого потерпілого до факту обману відносно нього або його ставлення до того, що в результаті висловлення власної довіри до певної особи (осіб) він був ошуканий.

Специфіка предмету шахрайства обумовлена закономірним зв'язком з особою потерпілого. У багатьох випадках при вчиненні шахрайства, особливо під час його підготовки, злочинець, оцінюючи реальну ситуацію, в якій йому доведеться діяти або в якій він уже діє, не може не враховувати вік, стать, фізичну силу, інтелектуальні можливості та інші індивідуальні якості потерпілого. Зв'язок «злочинець – потерпілий» виникає як наслідок розвитку злочинної події та дій особи, що вчинила злочин, і її взаємодії з потерпілим. Акт злочинного посягання перетворює існуючий до цього зв'язок заданих осіб (який мав особистий, побутовий або інший характер) у зв'язок кримінальний. У разі якщо злочинець і потерпілий до посягання не зустрічалися, не були знайомі, в основі розвитку зв'язку лежить лише факт учинення кримінального правопорушення.

Поведінка потерпілого може проявлятися у різних проявах: від повної віктимності, уразливості до впливу шахрая, нейтрального ставлення до останнього або активної протидії йому. Саме тому, що часто потерпілі самі провокують вчинення відносно них обманних дій, і відбувається подія кримінального правопорушення.

Віктимність поведінки потерпілих виражена не лише у довірливості відносно з іншими людьми чи у наявності негативних соціальних характеристик. Іноді самі власники майна створюють всі підстави для вчинення стосовно них шахрайства, наприклад, купують певне за надто заниженими цінами, майно за значно заниженими цінами, не звертають уваги на інформацію про власника повідомлення (наявність установчих даних, телефону), користуються під час купівлі підозрілими сайтами і т. ін.

Постраждати від шахрайства може практично кожен. Але існують певні характерні соціально-психологічні властивості особистості або їх комплекси, які можуть спричиняти віктимізацію особи стосовно шахрайства. Деякі дослідники, зокрема, зазначають, що підвищена віктимність у зв'язку з психологічними особливостями здебільшого притаманна саме потерпілим від шахрайства.

Природа вчинення шахрайства, з використанням ЕОТ, передбачає тривалий вербальний або конклюдентний контакт, або контакт в комплексі між потерпілим та злочинцем. Результатом такого контакту є введення першого в оману або маніпулювання його довірою. Тому вивчення зв’язку «потерпілий – злочинець» необхідне для побудування повної криміналістичної характеристики кримінального правопорушення, обрання тактики проведення окремих слідчих (розшукових) дій.

Залежно від наявності й впливу різних відносин, що існували або утворилися між злочинцем і потерпілим до вчинення кримінального правопорушення, проводиться розділення зв’язку за обставинами його утворення. Зв’язок за обставинами його утворення є залежним від наявності й впливу різних соціальних відносин, що існували або утворилися між злочинцем та потерпілим до або в момент вчинення кримінального правопорушення, і характеру їх розвитку. За обставинами утворення зв’язок буває такий, що: 1) розвинувся в результаті певних взаємин, які існували між злочинцем і його жертвою до вчинення кримінального правопорушення; 2) виник у результаті гостроконфліктної ситуації безпосередньо до або в момент вчинення кримінального правопорушення; 3) виник за відсутності якихось конфліктних взаємин між жертвою і злочинцем до вчинення кримінального правопорушення. Взаємини між майбутнім злочинцем і майбутнім потерпілим за своїм характером можуть бути різними: від хороших (близьких, інтимних, дружніх, приятельських) або таких, що мають байдужний, нейтральний характер, до неприязних, відверто ворожих.

Враховуючи, що особистість жертви шахрайства становить інтерес, насамперед, з точки зору її віктимного потенціалу стосовно цього кримінального правопорушення, в її соціально-психологічному дослідженні, окрім вже названих, можна визначити певні додаткові орієнтири. Це, зокрема, соціальнопсихологічні

чинники зниження критичності, обачності особи. Саме необачна поведінка властива переважній більшості жертв шахрайства. При цьому необачність слід розглядати не лише як сутнісну (сталу) властивість особистості, але і як одну з ознак поведінки у конкретній ситуації, яка залежить з одного боку від соціального досвіду особи, її поінформованості, звичок, інших особистісних властивостей, а з іншого – від впливу елементів зовнішнього середовища, у якому потенційна жертва опиняється у конкретний момент часу.