МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Юридичний факультет
Кафедра економічної безпеки та фінансових розслідувань

ТЮЛЮКІНА Оксана Володимирівна

Протидія економічним злочинам, що вчиняються в кіберпросторі / Counteraction to economic crimes committed in cyberspace

спеціальність: 262 – Правоохоронна діяльність
магістерська програма –Економічна безпека та фінансові розслідування

Магістерська робота

Виконала студентка групи
ПДЕБзм-21
О.В. Тюлюкіна
_____

Науковий керівник:
к.ю.н., доцент Н.Б. Москалюк
_____

Магістерську роботу допущено
до захисту:

«____» _____20__ р.

Завідувач кафедри

_____ Н.Б. Москалюк

ТЕРНОПІЛЬ - 2018

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Високі темпи розвитку інформаційних технологій, активне впровадження створюваних інформаційно-телекомунікаційних систем і технічних засобів в усі сфери життєдіяльності суспільства, а також сучасний стан систем захисту інформації створило об'єктивні передумови виникнення нового різновиду злочинів - злочинів у сфері високих технологій, поширення яких неминуче ставить співробітників правоохоронних органів перед необхідністю детального вивчення технічних можливостей існуючих комп'ютерних систем, їх використання в боротьбі зі злочинністю в даній сфері.

Так, сучасні комп'ютерні системи використовуються практично у всіх сферах науки, соціальної структури і, особливо, економіки. Відносна доступність інформаційних ресурсів, висока швидкість обробки баз даних, формування глобального кіберпростору - все це сприяє інтеграції інформаційних технологій в життя людини. Попри величезну кількість позитивних можливостей, які прийшли в життя кожної людини із перенесенням суспільних відносин в кіберпростір, все ж є і певні негативні – йдеться про кіберзлочинність, яка розвивається такими ж шаленими темпами, що й сам кіберпростір.

У зв'язку з цим боротьба та протидія злочинності в кіберпросторі є однією з актуальних проблем діяльності правоохоронних органів не лише України, а й кожної розвинутої держави зокрема.

Серед відомих на сьогоднішній день злочинів, скоєних в мережі Інтернет, особливу небезпеку становлять економічні злочини. В силу своєї високої латентності, а також труднощами виявлення і розслідування, дані злочини потребують всебічного наукового дослідження та обґрунтування можливостей протидії.

Зростання числа Інтернет-магазинів та Інтернет-аукціонів, створення систем надання банківських послуг в глобальній мережі, розвиток платіжних систем сприяє тому, що все більше і більше людей довіряють і користуються

розрахунками в кіберпросторі, забуваючи про те, що навіть у віртуальних економіках можуть скоюватися велика кількість злочинів

Сучасний стан наукової розробки питань методики розслідування та протидії економічним злочинам в мережі Інтернет характеризується, з одного боку, недостатнім інтересом до конкретного даного виду злочинів у порівнянні, скажімо, з кібертероризмом, поширенням порнографічної продукції чи порушенням інформаційної безпеки держави, а з іншого - великій теоретичній і практичній значимості для практики боротьби зі злочинами, вчиненими в мережі Інтернет. Все це знайшло своє відображення в дисертаційних дослідженнях таких національних вчених як Кравцова М. О., Козак Н.С., В.Г. Хахановський, Діордіца І. В., Буяджи С.А. та інших вчених.

Незважаючи на велику кількість публікацій, присвячених розслідуванню злочинів, пов'язаних з використанням комп'ютерної техніки, що з'явилися останнім часом, питання методики розслідування саме економічних злочинів в кіберпросторі практично не розглядалися. Більшість опублікованих на сьогоднішній день робіт, якщо і згадують про економічні злочини, то побіжно, частіше зупиняючись на дослідженні таких злочинів, як неправомірний доступ до комп'ютерної інформації, що врегульовані на сьогодні розділом 16 КК України.

Таким чином, актуальність обраного нами дослідження зумовлена, з одного боку, високою практичною значущістю, а з іншого - недостатньою науковою розробленістю питань методики розслідування економічної злочинності в кіберпросторі.

Об'єктом дослідження є криміналістична характеристика економічних злочинів в кіберпросторі, протиправна діяльність кіберзлочинців, а також особливості розслідування зазначеного виду злочину.

Предметом дослідження є закономірності формування загальної методики розслідування, а також використання спеціальних знань в сфері комп'ютерної інформації та високих технологій при розслідуванні економічних злочинів, вчинених із застосуванням глобальної мережі Інтернет.

Метою дослідження є розгляд теоретичних і практичних питань створення загальної методики розслідування економічної злочинності в кіберпросторі, що відповідає сучасному рівню розвитку високих інформаційних технологій, використання спеціальних знань в сфері комп'ютерної інформації та високих технологій при розслідуванні корисливих злочинів, пов'язаних з використанням мережі Інтернет, розробка науково обґрунтованих рекомендацій і раціональних способів організації взаємодії слідчого з спеціалістами та експертами і застосуванні зазначених спеціальних знань.

Для досягнення зазначеної мети сформульовані такі **основні завдання:**

- здійснити загальну характеристику економічних злочинів, що вчиняються в кіберпросторі;

- дослідити обстановку та спосіб вчинення злочинів;

- провести характеристику особистості типового злочинця;

- дослідити загальну характеристику кола потерпілих від економічних злочинів, що вчиняються в кіберпросторі;

- вивчити особливості проведення окремих оперативно-розшукових заходів;

- сформувати тактичні особливості допиту обвинуваченого та потерпілого від економічних злочинів, що вчиняються в кіберпросторі, також тактику обшуку;

- охарактеризувати процесуальні та непроцесуальні форми використання спеціальних знань;

- сформувати авторське бачення перспектив вирішення проблем у сфері розслідування та протидії економічній злочинності в кіберпросторі.

Методологічною основою дослідження є діалектична теорія пізнання, формальна логіка, криміналістична методологія і загальнотеоретичні концепції криміналістики. У дослідженні використані загальнонаукові методи пізнання (аналіз, синтез, статистичний метод), а також методи інших наук, зокрема основи теорії інформаційної безпеки.

Наукова новизна одержаних результатів. У дослідженні сформульовані наступні висновки та рекомендації, що відзначаються науковою новизною:

- надані авторські визначення обстановки вчинення економічних злочинів у кіберпросторі, а також спеціальних знань, які використовуються при розслідуванні даного виду злочинів;

- сформульовано рекомендації щодо напрямів взаємодії слідчого з експертами та спеціалістами при проведенні оперативно-розшукових заходів і слідчих дій при розслідуванні злочинів, пов'язаних з використанням засобів комп'ютерної техніки;

- доведено, що власні знання слідчого в сфері високих технологій в більшості випадків можуть виявитися недостатніми для самостійного дослідження комп'ютерної техніки. Навіть якщо слідчий володіє необхідними спеціальними знаннями, необхідне залучення експерта або спеціаліста для надання висновку, оскільки кримінально-процесуальне законодавство забороняє суміщення двох процесуальних ролей в одній особі.

Практичне значення дослідження полягає в тому, що розроблені в магістерській роботі наукові положення і практичні рекомендації покликані сприяти підвищенню ефективності правозастосовчої діяльності правоохоронних органів. Пропозиції та рекомендації, зроблені за результатами проведеного дослідження, можуть застосовуватися у викладанні дисциплін кримінально-процесуального спрямування у вищих навчальних закладах, а також при підготовці або підвищенні кваліфікації працівників правоохоронних органів.

Апробація результатів дослідження. Результати дослідження знайшли відображення у доповіді на Всеукраїнській науково-практичній конференції «Тактичні та стратегічні пріоритети зміцнення фінансово-економічної безпеки держави». – Тернопіль, 2018.

Структура магістерської роботи. Дослідження складається зі вступу, трьох розділів, 10 підрозділів, висновків та списку використаних джерел. Загальний обсяг роботи становить 121 сторінку, кількість використаних джерел – 115.

РОЗДІЛ 1. ПОНЯТТЯ ТА ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЕКОНОМІЧНИХ ЗЛОЧИНІВ, ЩО ВЧИНЯЮТЬСЯ В КІБЕРПРОСОРІ

1.1. Загальна характеристика економічних злочинів, що вчиняються в кіберпросторі: криміналістичний аспект

Перш ніж перейти до безпосереднього висвітлення питання економічних злочинів у кіберпросторі, необхідно визначитись у понятійно-категоріальному апараті, тобто дослідити що саме під якими термінами ми розуміємо. Отож, в першу чергу необхідно визначитись із категорією «економічні злочини».

Науковий інтерес до поняття економічної злочинності викликаний тим, що у вітчизняній літературі існує диференційований підхід до визначень злочинів у сфері економіки. Розмаїття тлумачень даного явища зустрічається у наукових дослідженнях багатьох вчених, зокрема виділяють «злочини у сфері економіки», «економічні злочини», «тіньова економіка», «кримінальна економіка», «економічна злочинність» та інші. Дані поняття часто ототожнюють, однак мають місце спроби доведення різної природи наведених явищ.

В енциклопедії сучасної України економічні злочини розглядаються як різновид злочинів, здійснюваних у процесі професійної діяльності в рамках і під прикриттям законної економічної діяльності з використанням легальних економічних інститутів (правил, форм, процедур). Економічна злочинність є основою тіньової економіки і спрямована на майнові та виробничі відносини, економічні права громадян, юридичних осіб, муніципальних і державних утворень [34].

Н. С. Козак розглядає економічний злочин як майновий і корисливий злочин, а також злочин у сфері економіки, автор зазначає, що економічна злочинність характеризується сукупністю корисливих зазіхань на власність, порядок управління народним господарством, що вчиняється особами, які займають певні соціальні позиції в структурі економіки [49, с. 484].

На думку С. Кравчука усі ці поняття мають різний спектр вчинення протиправних діянь. Так, злочини у сфері економіки, як стверджує автор, це переважно господарські злочини, які вчиняються в різних сферах; економічна

злочинність полягає у вчиненні злочинів у сфері господарської діяльності, в тому числі із використанням службового становища. До злочинів економічного характеру С. Кравчук відносить діяння, які пов'язані із спричиненням матеріальної шкоди чи отримання матеріальної вигоди [58].

Ми з останньою думкою цілком погоджуємось, оскільки також вважаємо, що поняття «економічного злочину» має мати розширене трактування і включати не лише злочини у сфері господарської діяльності, що виділені чинним КК України в окремий розділ, а й інші злочини майнового характеру.

Зважаючи на таке розширене тлумачення, варто відзначити, що кримінальне законодавство містить у собі велику групу норм, які визначають кримінальність діянь у сфері економічної діяльності і юридичну відповідальність за їх скоєння. Вони об’єднані в самостійні розділи «Злочини у сфері господарської діяльності» та «Злочини проти власності».

Кожен із названих розділів містить доволі значну кількість норм, які визначають діяння злочинними. Скажімо Розділ VI «Злочини проти власності» містить 16 статтей і передбачає відповідальність за такі суспільно-небезпечні діяння: Крадіжка; Грабіж; Розбій; Викрадення води, електричної або теплової енергії шляхом її самовільного використання; Вимагання; Шахрайство; Привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем; Заподіяння майнової шкоди шляхом обману або зловживання довірою; Незаконне привласнення особою знайденого або чужого майна, що випадково опинилося у неї; Умисне знищення або пошкодження майна; Умисне пошкодження об'єктів електроенергетики; Погроза знищення майна; Необережне знищення або пошкодження майна; Порушення обов'язків щодо охорони майна; Самовільне зайняття земельної ділянки та самовільне будівництво; Придбання, отримання, зберігання чи збут майна, одержаного злочинним шляхом [60].

Тоді як Розділ VII «Злочини у сфері господарської діяльності » містить 34 статті і встановлює кримінальну відповідальність за: Виготовлення, зберігання, придбання, перевезення, пересилання, ввезення в Україну з метою

використання при продажу товарів, збуту або збут підроблених грошей, державних цінних паперів, білетів державної лотереї, марок акцизного податку чи голографічних захисних елементів; Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення; Контрабанда; Незаконний обіг дисків для лазерних систем зчитування, матриць, обладнання та сировини для їх виробництва; Зайняття грального бізнесом; Незаконне виготовлення, зберігання, збут або транспортування з метою збуту підакцизних товарів; Фіктивне підприємництво; Підроблення документів, які подаються для проведення державної реєстрації юридичної особи та фізичних осіб - підприємців; Протидія законній господарській діяльності; Протиправне заволодіння майном підприємства, установи, організації; Легалізація (відмивання) доходів, одержаних злочинним шляхом; Умисне порушення вимог законодавства про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансування; Нецільове використання бюджетних коштів, здійснення видатків бюджету чи надання кредитів з бюджету без встановлених бюджетних призначень або з їх перевищенням; Видання нормативно-правових актів, що зменшують надходження бюджету або збільшують витрати бюджету всупереч закону; Ухилення від сплати податків, зборів (обов'язкових платежів); Ухилення від сплати єдиного внеску на загальнообов'язкове державне соціальне страхування та страхових внесків на загальнообов'язкове державне пенсійне страхування; Порушення порядку здійснення операцій з металобрухтом; Незаконне виготовлення, підроблення, використання або збут незаконно виготовлених, одержаних чи підроблених контрольних марок; Доведення банку до неплатоспроможності; Доведення до банкрутства; Порушення порядку ведення бази даних про вкладників або порядку формування звітності; Фальсифікація фінансових документів та звітності фінансової організації, приховування неплатоспроможності фінансової установи або підстав для відкликання (анулювання) ліцензії

фінансової установи; Шахрайство з фінансовими ресурсами; Маніпулювання на фондовому ринку; Підроблення документів, які подаються для реєстрації випуску цінних паперів; Порушення порядку ведення реєстру власників іменних цінних паперів; Виготовлення, збут та використання підроблених недержавних цінних паперів; Умисне введення в обіг на ринку України (випуск на ринок України) небезпечної продукції; Незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару; Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю; Розголошення комерційної або банківської таємниці; Незаконне використання інсайдерської інформації; Приховування інформації про діяльність емітента; Незаконна приватизація державного, комунального майна [60].

Всі вищевказані злочинні діяння об’єднує мета спричинення матеріальної шкоди чи отримання матеріальної вигоди. Та оскільки основна мета нашого дослідження – вивчити економічну злочинність у кіберпросторі, то серед вказаних злочинів обох розділів ми маємо відшукати тих, які можуть здійснюватися в мережі Інтернет. Для цього серед диспозицій статей шукатимем ті злочинні діянні, де кваліфікуючою ознакою буде використання електронно-обчислювальної техніки.

Провівши детальний аналіз усіх вищевказаних злочинних діянь, ми виявили, що попри величезну кількість статей із злочинним економічним спрямуванням, на думку нашого законодавця лише ст. 190 у ч. 3 передбачає кримінальну відповідальність за шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки, а також ст. 200 КК України, що кримінально караним визнає незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення. Тобто є лише два види злочинних діянь економічного спрямування, що можуть вчинятись в кіберпросторі.

Розглянемо детальніше кожне із них:

Варто відзначити, що розуміння шахрайства чинним КК України бере свій початок ще із КК РРФСР 1922 та 1960 року. Так, скажімо в КК РРФСР 1960 року під шахрайством розумілося заволодіння особистим майном громадян або придбання права на майно шляхом обману чи зловживання довірою.

В чинному Кримінальному кодексі України шахрайством визначено заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою. Іншими словами, суть кримінально-караного діяння не змінилась, лише те що до 2001 року трактувалось як особисте майно громадян тепер має лаконічнішу і ширшу форму – чуже майно. То ж під цим майном вже можна розуміти і майно громадян, і іноземних громадян чи осіб без громадянства, і що важливо юридичних осіб чи держави. Тобто зі зміною редакції КК України суттєво розширилась сфера потенційних потерпілих від шахрайства.

Обман і зловживання довірою як способи шахрайства усвідомлюються як досягнення певних проміжних результатів перед остаточним отриманням чужого майна або отриманням права на нього, а саме введення в оману власника майна таким чином, щоб злочинець згодом сам отримав майно від жертви. В іншому випадку, це буде не шахрайство, а різновид крадіжки, скоєної з застосуванням спеціальних методів [10, с. 54].

В останні роки активний розвиток отримало шахрайство в мережі Інтернет. Звісно ж, що основна відмінність даного виду злочинів від традиційного шахрайства полягає в особливій обстановці вчинення злочинного посягання.

Інтернет-шахрайство, яке, з одного боку, є результатом еволюції традиційного шахрайства, оскільки деякі його види зустрічаються в Інтернеті без будь-яких серйозних змін в методиці реалізації злочинного замислу; з іншого боку - це якісно нова група злочинів, оскільки при схожості методів реалізації, конкретні способи мають істотні відмінності [59, с. 41]. Цей різновид злочинів, як і багато інших комп'ютерних злочинів, характеризується високою латентністю, по-перше, через складність розслідування, а по-друге, через специфіку реалізації шахрайських схем в Інтернеті.

Як і в традиційному шахрайстві, тут основна маса посягань направлена на невизначено широке коло потенційних жертв.

Однією з особливостей є також те, що для деяких способів інтернет-шахрайства характерна наявність додаткових вимог до особистості злочинця. Найчастіше мова йде про наявність спеціальних знань у певній сфері - сфері інформаційних технологій.

Звісно ж, що у випадку з інтернет-шахрайствами посягання відбувається виключно на право на майно, оскільки Інтернет є, скоріше, певним середовищем здатним до передачі виключно інформації. Таке середовище можна вважати матеріальним лише умовно, оскільки вона не має всі ознаки матеріальності. На наш погляд, в даному випадку доречно говорити про віртуальному світі і віртуальному середовищі, яка, будучи об'єктом матеріального світу, проте, нематеріальна.

Таким чином, якщо злочинець, зробивши щодо невизначеної великої групи людей шахрайство, викрав їх грошові кошти, перевівши їх на свій таємний банківський рахунок, то це, на наш погляд, не буде розкраданням саме грошових коштів. Швидше навпаки, це повинно вважатися отриманням права на них, в тому числі права отримати ці гроші в матеріальній формі (наприклад, перевести в готівку через банкомат).

Перш ніж приступити до більш детального розгляду шахрайства в мережі Інтернет, необхідно дати характеристику з криміналістичної точки зору шахрайства взагалі.

Аналізуючи різні підходи до вирішення питання про зміст поняття криміналістичної характеристики шахрайства, можна виділити наступні елементи, що найчастіше вказуються дослідниками:

1) обстановка вчинення злочину, в тому числі місце і час, а також обставини, що сприяли вчиненню злочину;

2) спосіб вчинення злочину (спосіб підготовки, спосіб безпосереднього здійснення і спосіб приховування скоєного);

3) об'єкт і предмет посягання;

4) загальна характеристика особистості злочинця;

5) загальна характеристика особистості потерпілого.

Запорукою успішної і найбільш ефективної реалізації злочинного задуму є правильний вибір часу і місця вчинення злочину. Тому деякі автори обґрунтовано роблять висновок, що в тих місцях, де найчастіше відбуваються деякі види шахрайства (наприклад, на вокзалах або в інших місцях великого скупчення людей), необхідно проводити заходи, спрямовані на попередження вчинення цих злочинних дій.

При плануванні злочину враховуються і такі чинники, як соціально-економічна обстановка, природно-кліматичні особливості території, на якій збирається діяти шахрай, та інше. Зокрема, аналіз цих факторів дозволяє вибрати такий спосіб дії, який дозволить, з одного боку, забезпечити максимальне прикриття, а з іншого - отримати найбільший прибуток від більшої кількості потенційних жертв.

Звісно ж, що вміння адекватно оцінювати соціально-економічнуобстановку є одним з найнебезпечніших якостей у шахрая. Як показує історія, найуспішніші фінансові піраміди створювалися саме такими людьми. Спосіб вчинення злочину є основним елементом всієї криміналістичної характеристики будь-якого злочину. У загальному вигляді його можна визначити як сукупність дій, спрямованих на реалізацію злочинного задуму. Дана сукупність носить системний характер і утворює три взаємопов'язані етапи:

1) дії підготовчого характеру, спрямовані на створення умов, що роблять можливим і / або найменш важким подальшу реалізацію злочинного задуму;

2) дії щодо безпосередньої реалізації злочинцем задуманого;

3) дії, спрямовані на приховування слідів злочину і перешкоджання його виявлення і розслідування правоохоронними органами.

З точки зору криміналістики, важливі всі три етапи, однак в даній роботі найбільший інтерес представляє другий етап, за яким в деяких випадках також відбувається кримінально-правова кваліфікація (наприклад, вбивство, вчинене суспільно небезпечним способом). До того ж, як зазначається в літературі, встановивши і проаналізувавши спосіб вчинення злочину, можна не тільки

зробити висновок про те, які можливі підготовчі дії були вчинені, а також які типові сліди слід шукати [26].

Наприклад, І.О. Громико пише, що «знання типових слідів, які залишаються в обстановці, якщо злочинець для вчинення злочину скористався даними способом, особливо корисні на початковому етапі розслідування, коли відчувається дефіцит вихідних даних про злочин. Ці знання допомагають вести цілеспрямований пошук реально існуючих слідів і в міру їх виявлення конкретизувати уявлення про спосіб вчинення злочину, який належить розслідувати. Підтвердження відомостей про спосіб вчинення злочину дозволить спланувати подальші заходи, конкретизувати методику його розслідування » [29, с.36].

Таким чином, вивчення безпосередніх способів здійснення інтернет-шахрайства, їх особливостей, еволюції і т.д. дозволить слідчому більш ефективно діяти на ранніх стадіях розслідування і, зокрема, дасть можливість зібрати максимально можливу кількість інформації, корисної для подальшого розслідування.

Отже, дії шахрая, в якому б вигляді вони не були виражені (тобто, який би не був обраний злочинцем спосіб досягнення своїх цілей), завжди залишають певні сліди, в ролі яких можуть виступати різні об'єкти (наприклад, фальшиві документи).

Звісно ж, що оскільки будь-яка дія залишає свій слід, то можна зробити висновок, що аналіз слідів тих дій, які спрямовані на приховування слідів злочину, дозволить з'ясувати, які саме сліди були приховані. Потрібно, однак, врахувати, що в даному випадку необхідно проводити аналіз цілої групи однотипних злочинів для визначення належності слідів, що залишилися після приховування скоєного, до тих чи інших злочинів.

З огляду на те, що стаття про шахрайство знаходиться в розділі КК України про злочини проти власності, то родовим об'єктом даного складу злочину є охоронювані законом відносини в сфері економіки, а видовим - охоронювані законом відносини власності.

Предметом шахрайства, виходячи з тексту статті 190 КК України, є чуже майно або право на чуже майно. Оскільки законодавець розглядає шахрайство як одну з форм розкрадання, то вказівка в статті права на чуже майно, в якості одного з предметів посягання, відображає специфіку даного злочину на тлі, наприклад, звичайної крадіжки (її предметом не може бути право на майно).

Таким чином, оскільки законодавець не робить уточнень з приводу предмета шахрайства, таким можна вважати і рухоме, і нерухоме майно або право на це майно.

У більшості випадків безпосереднім предметом шахрайства є грошові кошти, які, в силу свого особливого статусу, становлять найбільший інтерес для шахраїв. Решту предметів, здебільшого, також можна умовно прирівняти до грошей, так як, в кінцевому рахунку, після розкрадання або придбання права на них, це майно потім перепродується.

Крім грошей предметом шахрайства можуть бути також, наприклад, коштовності і предмети розкоші, транспортні засоби, програмне забезпечення для комп'ютерів і інших електронно-обчислювальних пристроїв, побутові прилади, одяг, земельні ділянки та будівлі на них, інше рухоме і нерухоме майно.

Оскільки КК України [60] не містить докладної інформації про те, що необхідно розуміти під правом на майно в контексті його (кодексу) статей, то може виникнути питання про те, чи вважати злочин закінченим з моменту отримання повного права власності на майно, або ж мова йде тільки про якусь певну правомочність (володіння, користування або розпорядження).

Звісно ж, що це питання має вирішуватися в кожному конкретному випадку. Оскільки права на майно (а також обсяг цих прав) закріплюються у відповідних документах, то в випадках, коли предметом злочинного посягання є право на чуже майно, злочин має вважатися завершеним з того моменту, коли злочинець наділяється тим обсягом прав, яким, на підставі відповідних документів, була наділена жертва, або, як виняток, в тому обсязі, в якому це необхідно для здійснення будь-яких дій з майном (наприклад, купівля-продаж).

Деякі дослідники вважають, що при вивченні шахрайства вивчення особистості злочинця має особливе значення [38, с. 100]. Представлені в криміналістичній літературі точки зору на особистість шахрая можна умовно розділити на дві групи.

Представники першої групи вважають, що шахрайство як злочин вимагає від злочинця наявності сукупності спеціальних якостей: гострий розум, широкий кругозір, хороша реакція, товариськість, вміння заручитися підтримкою, відмінне знання людської психології та т.д. Наприклад, Карчевський М. В. характеризує шахраїв як «висококваліфікованих професіоналів, що володіють широким кругозором і знаннями в сфері права», вважаючи, що для шахрая характерне «виховання або розвиток вміння імпровізувати, оперативно реагувати на швидко мінливу обстановку» [42, с. 47]. Н.С. Козак описує про шахраїв як «еліту злодійського світу» [50, с. 15]. Схожих поглядів дотримуються і деякі інші дослідники.

Іншої позиції дотримуються представники другої групи. Зокрема, вони вважають, що шахрайство здатне зробити будь-яка людина, і що злочинності в даній сфері сприяє ситуація, що склалася, але ніяк не особливі риси особистості [57]. Ми, однак, не згодні з тими вченими, хто вважає, що шахрайство може зробити абсолютно будь-яка людина. На наш погляд, в даному випадку необхідно враховувати такі фактори як виховання, система внутрішніх цінностей і деякі інші. Можна погодитися з думкою, що кожна людина здатна до скоєння злочину взагалі, але ніяк не шахрайства, зокрема.

Звісно ж, що обидві описані точки зору мають право на життя, нехай і з деякими застереженнями, оскільки в даний час існує величезна кількість різних видів шахрайства, і деякі з них не вимагають від злочинця наявності будь-яких особливих особистісних якостей. Також, на наш погляд, можна погодитися з тими дослідниками, хто називає шахраїв «елітою злодійського світу», бо метою шахрая є таке розкрадання, при якому жертва, навіть коли усвідомлює, що втратила майнj, не завжди буде в першу чергу думати про те, що стала жертвою злочинця.

Слід зазначити, що традиційні види шахрайства характеризуються високим відсотком рецидиву. Тому серед шахраїв дуже багато тих, хто вже притягувався до кримінальної відповідальності. При цьому велика частина рецидивістів раніше притягувалася до відповідальності за вчинення корисливих злочинів, в тому числі і шахрайства. Примітною особливістю, як зазначається в літературі, є те, що багато рецидивісти спеціалізуються на якомусь одному виді шахрайства [64].

Ми вважаємо, що подібне явище має місце через особливості особистості шахрая. Вибір кращого способу вчинення злочину залежить від наявності, відсутності і розвиненості тих чи інших особистісних якостей. Злочинець зіставляє те, що він хоче, і те, що він може зробити для досягнення бажаного результату. Після цього він вибирає найбільш оптимальний спосіб дії, який потім в своїй основі не змінюється. Деякі види шахрайства настільки складні у виконанні, що вимагають більш вузької спеціалізації. У таких випадках дуже часто злочинці діють спільно, утворюючи групи за попередньою змовою або організовані групи. Особливу небезпеку становлять останні, про що свідчить згадка про організовані групи в частині 4 ст. 190 КК України.

Організовані злочинні групи характеризуються найвищим ступенем згуртованості і розподілу ролей. Такі об'єднання утворюються з метою багаторазового вчинення актів шахрайства на певній території. Тому при розслідуванні таких злочинів необхідно враховувати, що у злочинців можуть бути корупційні зв'язки з місцевими правоохоронними органами, а також і з представниками влади.

В останні роки простежується чітка тенденція «зрощування» реального злочинного світу і так званим віртуальним. В контексті дослідження шахрайства в мережі Інтернет можна сказати, що така тенденція, в кінцевому рахунку, дозволить будувати більш складні шахрайські схеми. Як наслідок, суттєво зростає складність виявлення і розслідування таких злочинів і, як нам представляється, можливі конфлікти підслідності, коли різні правоохоронні органи будуть розслідувати один злочин.

Щоб вирішити цю проблему необхідно не тільки вдосконалити механізм формування слідчих груп, а й передбачити систему обміну інформацією між правоохоронними органами з метою підвищення ефективності дій їхніх співробітників на ранніх стадіях розслідування злочину.

Потерпілими від шахрайства, виходячи з положень статті 55 КПК України, може бути як фізична особа, якій кримінальним правопорушенням завдано моральної, фізичної або майнової шкоди, так і юридична особа, якій кримінальним правопорушенням завдано майнової шкоди [61].

Звісно ж, основна частина цих злочинів скоєно в відношенні окремих людей.

Потерпілих від шахрайства можна класифікувати виходячи з активності їхньої поведінки після отримання інформації про те, що вони стали жертвами шахраїв. За цією ознакою виділяються наступні основні групи:

1. Потерпілі, зацікавлені в успішному розслідуванні злочину, надають правоохоронним органам всю відому їм інформацію і здійснюють активне сприяння в інших формах.

2. Потерпілі з пасивною поведінкою. Представники цієї групи, як правило, обмежуються подачею заяви і не стежать за ходом розслідування, або взагалі не вживають будь-яких дій для залучення шахраїв до кримінальної відповідальності.

Виділяють також ще одну групу потерпілих, представники якої схильні приховувати свій статус, і навіть, в деяких випадках, надавати протидію правоохоронним органам у веденні розслідування. Це можуть бути як фізичні, так і юридичні особи. Причини такої, на перший погляд, нелогічної поведінки криються, найчастіше, в страху: страх за ділову репутацію, страх розкриття деяких аспектів особистого життя і т.д.

Звісно ж, що дана група може виступати як один із критеріїв визначення рівня латентності того чи іншого злочину. Комп'ютерні злочини взагалі і інтернет-шахрайство, зокрема, спочатку мають досить високий рівень латентності. Для вирішення даної проблеми ми пропонуємо проводити роботу з підвищення довіри до правоохоронних органів. Це дозволить не тільки

збільшити кількість виявлених порушень, а й залучати більшу кількість потерпілих до співпраці в розслідуванні, а також оперувати більш повною інформацією і, отже, більш якісно розслідувати інтернет-шахрайства. Проведення такої роботи особливо актуально для попередження злочинів, пік здійснення яких припадає на певну пору року. У таких випадках роботи з інформування дозволять звертати увагу населення на поточну кримінальну обстановку і тримати в курсі про найбільш серйозні загрози на даний момент.

Підводячи проміжний підсумок, можна зробити наступні висновки:

1. Основними елементами криміналістичної характеристики шахрайства в мережі Інтернет є такі:

1) обстановка вчинення злочину, в тому числі місце і час;

2) спосіб вчинення злочину (спосіб підготовки, спосіб безпосереднього здійснення і спосіб приховування скоєного);

3) об'єкт і предмет посягання;

4) загальна характеристика особистості злочинця;

5) загальна характеристика особистості потерпілого.

2. Обман і зловживання довірою як способи шахрайства є досягненням певних проміжних результатів перед остаточним отриманням чужого майна або отриманням права на нього, а саме введення в оману власника або власника майна таким чином, щоб злочинець згодом саме отримав майно від жертви. В іншому випадку, це буде не шахрайство, а різновид крадіжки, скоєної з застосуванням спеціальних методів.

3. При здійсненні інтернет-шахрайства посягання відбувається виключно на право на майно, оскільки Інтернет є, скоріше, середовищем, здатним до передачі виключно інформації. Таке середовище можна вважати матеріальним лише умовно, оскільки воно не має всіх ознак матеріальності. В даному випадку доречно говорити про віртуальний світ і віртуальне середовище, яке, будучи об'єктом матеріального світу, проте, нематеріальне.

4. У більшості випадків безпосереднім предметом шахрайства є грошові кошти, які, в силу свого особливого статусу, становлять найбільший інтерес для шахраїв. Решту предметів, здебільшого, також можна умовно прирівняти до

грошей, так як, в кінцевому рахунку, після розкрадання або придбання права на них, це майно потім перепродується.

5. Оскільки КК України не містить докладної інформації про те, що необхідно розуміти під правом на майно в контексті його статей, то може виникнути питання про те, чи вважати злочин закінченим з моменту отримання повного права власності на майно, або ж мова йде тільки про якусь правомочність (володіння, користування або розпорядження).

Звісно ж, що це питання має вирішуватися в кожному конкретному випадку. Оскільки права на майно (а також обсяг цих прав) закріплюються у відповідних документах, то в випадках, коли предметом злочинного посягання є право на чуже майно, злочин має вважатися завершеним з того моменту, коли злочинець наділяється тим обсягом прав, яким, на підставі відповідних документів, була наділена жертва, або, як виняток, в тому обсязі, в якому це необхідно для виробництва будь-яких дій з майном (наприклад, купівля-продаж).

6. В останні роки простежується чітка тенденція «зрощування» реального злочинного світу і так званим віртуального. В контексті дослідження шахрайства в мережі Інтернет можна сказати, що така тенденція, в кінцевому рахунку, дозволить будувати більш складні шахрайські схеми. Як наслідок, суттєво зростає складність виявлення і розслідування таких злочинів.

7. Потерпілими від інтернет-шахрайства, виходячи із положень статті 42 КПК України, може бути як фізична особа, якій злочином заподіяно фізичну, майнову, моральну шкоду, так і юридична особа, якщо заподіяна шкода його майну або діловій репутації. Звісно ж, проте, що основна частина цих злочинів скоєно щодо окремих людей.

Аналізуючи другий вид економічних злочинів, що можуть здійснюватись в кіберпросторі, розглянемо ст. 200 КК України, яка вказує, що «Підробка документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, а так само придбання, зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ чи платіжних карток або їх використання чи збут - карається штрафом від п'ятисот до тисячі

неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до трьох років. 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, - караються позбавленням волі на строк від двох до п'яти років.

Примітка. Під документами на переказ слід розуміти документ в паперовому або електронному виді, що використовується банками чи їх клієнтами для передачі доручень або інформації на переказ грошових коштів між суб'єктами переказу грошових коштів (розрахункові документи, документи на переказ готівкових коштів, а також ті, що використовуються при проведенні міжбанківського переказу та платіжного повідомлення, інші) [60].

Об'єктом даного злочину є встановлений порядок виготовлення, використання та обігу документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, який забезпечує нормальне функціонування банківської системи України. Предметом злочину є: 1) документи на переказ грошових коштів; 2) платіжні картки; 3) інші засоби доступу до банківських рахунків.

Поняття документів на переказ дано у примітці до ст. 200. Такими документами, зокрема, є: а) розрахункові документи, якими є платіжне доручення, платіжна вимога-доручення, розрахунковий чек, платіжна вимога та розрахункові документи інших видів, встановлені НБ; б) міжбанківські розрахункові документи, тобто документи на переказ, сформовані банком на підставі поданих клієнтами розрахункових документів, документів на переказ готівки, а також доручень на договірне списання, передбачених в договорах, укладених між клієнтами та обслуговуючими їх банками; в) документи на переказ готівкових коштів, реквізити та особливості оформлення яких також встановлюються Національним банком України; г) клірингові вимоги; д) інші документи, що використовуються в платіжних системах для ініціювання переказу.

Платіжна картка - це спеціальний платіжний засіб у вигляді емітованої в установленому законодавством порядку пластикової чи іншого виду картки, що використовується для ініціювання переказу грошей з рахунка платника або з відповідного рахунка банку з метою оплати вартості товарів і послуг,

перерахування грошей зі своїх рахунків на рахунки інших осіб, отримання грошей у готівковій формі в касах банків, пунктах обміну іноземної валюти уповноважених банків та через банківські автомати, а також здійснення інших операцій, передбачених відповідним договором.

Іншими засобами доступу до банківських рахунків слід вважати будь-які, крім документів на переказ та платіжних карток, документи чи предмети, із застосуванням яких особа може з відома працівників банку отримати доступ до певного банківського рахунка та можливість здійснювати операції з коштами, які знаходяться на такому рахунку. Таким іншим засобом, зокрема, є банківська ідентифікаційна картка (ідентифікаційна картка) - ідентифікаційний засіб у вигляді пластикової чи іншого виду картки, що містить реквізити, визначені банком, які ідентифікують клієнта та його рахунки в банку.

При вчиненні цього злочину шляхом придбання, зберігання, перевезення, пересилання з метою збуту, використання чи збуту його предметом є лише підроблені документи на переказ чи підроблені платіжні картки.

Об’єктивна сторона злочину може виражатися у вчиненні будь-якої незаконної дії, передбаченої ч. 1 ст. 200 КК: а) у підробці документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, електронних грошей; б) у придбанні, зберіганні, перевезенні, пересиланні, використанні або збуті підроблених документів на переказ чи платіжних карток; в) у неправомірному випуску або використанні електронних грошей.

Підробка документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, електронних грошей - це створення повністю фальсифікованого предмета або часткова фальсифікація справжнього предмета.

Підробкою предметів цього злочину є будь-які дії, внаслідок яких створюються підроблені документи на переказ, платіжні картки чи інші засоби доступу до банківських рахунків, у т.ч. фальсифікація відповідних справжніх предметів, внаслідок якої з їх застосуванням можуть бути проведені незаконні (ініційовані не власником рахунка або не забезпечені наявністю грошей на банківському рахунку) перекази грошових коштів або ж доступ до інформації щодо певного банківського рахунка отримує неуповноважена на це особа.

Підробка може бути здійснена за допомогою спеціального технічного обладнання, комп'ютерних програмних засобів або у будь-який інший спосіб (дописка, підчистка, виправлення у паперових документах тощо).

Поняття придбання, зберігання, перевезення, пересилання, збуту, вжиті у цій статті, за своїм змістом збігаються з поняттями, застосованими у ст. 199 (див. коментар до ст. 199). Під використання підроблених документів на переказ чи платіжних карток слід розуміти пред'явлення їх як справжніх з метою здійснення незаконного переказу грошових коштів, незаконного доступу до інформації щодо відповідного банківського рахунка тощо. Використанням підробленої платіжної картки слід вважати також спробу отримання з ЇЇ допомогою грошових коштів через банківський автомат, здійснення з її застосуванням оплати товарів чи послуг.

Якщо внаслідок використання підроблених предметів особа, яка їх використала, заволодіває чужими грошовими коштами, вчинене слід кваліфікувати як сукупність злочинів за відповідними частинами ст. ст. 190 і 200.

Злочин, залежно від способу, є закінченим з моменту вчинення однієї із перелічених у ч. 1 ст. 200 дій.

Суб'єктом злочину може бути будь-яка особа віком від 16 років. Суб'єктивна сторона злочину характеризується прямим умислом. Обов'язковою ознакою підробки, придбання, зберігання, перевезення, пересилання відповідних предметів злочину є мета їх збуту.

Кваліфікуючими ознаками злочину є вчинення його; 1) повторно; 2) за попередньою змовою групою осіб.

Відносини щодо випуску та використання електронних грошей регулюються Законом України «Про платіжні системи і переказ коштів в Україні» від 5 квітня 2001 р., Положенням про електронні гроші в Україні, затвердженим постановою Правління НБУ від 4 листопада 2010 р. № 481, та іншими нормативними актами.

Випуск електронних грошей - це операція з уведення в обіг електронних грошей емітентом шляхом їх надання користувачам або комерційним агентам в

обмін на готівкові або безготівкові кошти. Електронні гроші є випущеними з часу їх завантаження емітентом або оператором на електронний пристрій, що перебуває в розпорядженні користувача або агента.

Випуск електронних грошей може здійснювати виключно банк. Останнім визнається юридична особа, яка на підставі банківської ліцензії має виключне право надавати банківські послуги, відомості про яку внесені до Державного реєстру банків. Банк, що здійснює випуск електронних грошей, бере на себе зобов'язання з їх погашення.

Неправомірність випуску електронних грошей полягає в тому, що він здійснюється суб'єктом, який не має права на випуск електронних грошей, тобто особою, яка не є банком. Порушення банком порядку здійснення операцій з електронними грошима, у тому числі порядку вчинення операції щодо їх випуску, тягне за собою адміністративну відповідальність за ст. 16314 КУпАП.

1.2. Обстановка та спосіб вчинення злочинів

На сьогоднішній день розгляду сферах науки: кримінально-процесуального права, криміналістики та кримінального права. Звісно ж, що перед тим як приступити до розгляду обстановки скоєння злочину з точки зору криміналістики і, зокрема, обстановки скоєння шахрайства в мережі Інтернет, необхідно проаналізувати підходи до визначення даного поняття в кримінальному праві, оскільки його норми як галузі законодавства і положення як галузі науки, є основоположними для криміналістики.

В даний час в науці кримінального права щодо поняття «обставини вчинення злочину» існує досить багато різних точок зору. Звісно ж, що основні з них зводяться до наступних. Згідно з однією з точок зору, в поняття обстановки скоєння злочину слід включати тільки ті ознаки, які характеризують злочин з зовнішньої сторони. Так, на думку М. Ю. Літвінова, під обстановкою вчинення злочину розуміють «сукупність об'єктивних умов, в яких протікав зовнішній акт злочинної поведінки» [65, с. 86].

Інше розуміння обстановки скоєння злочину розкрив О. В. Манджай, який трактує її у вузькому і широкому сенсі. У вузькому сенсі обстановка обмежена комплексом речей, явищ і процесів, що відбуваються в зовнішньому світі, а в більш широкому сенсі - включає в себе також місце, час та інші конкретні умови здійснення злочину [67, с. 79]. Розвиваючи далі свою точку зору, він вказував, що «обстановка вчинення злочину не зводиться до сукупності безпосередніх фізичних умов, в яких діє злочинець. Це поняття охоплює більш широке коло явищ і включає також загальну історичну і соціально-політичну обстановку, конкретні умови життя і діяльності даного колективу, в якому було скоєно злочин ».

Звісно ж, що вузький підхід до розуміння обстановки більше підходить для науки кримінального права, оскільки в ньому більш чітко простежується розмежування обстановки та інших ознак об'єктивної сторони складу злочину.

Найбільш повною і точною видається позиція Матусовского Г.А., який розглядає обстановку скоєння злочину як «обмежена просторово-часовими рамками вчиненого злочину взаємодія людини, матеріальних предметів, природно-кліматичних та інших факторів, що робить вплив на ступінь суспільної небезпеки вчиненого діяння і яка набуває в зв'язку з цим кримінально правового значення» [71 с. 56].

Основна фактична властивість обстановки полягає в її здатності впливати на процес вчинення злочинного діяння: на його основі визначається і кримінально-правове значення цієї ознаки, яке складається в здатності обстановки змінювати суспільну небезпечність вчиненого в її умовах діяння.

До елементів обстановки Никифорчук Д. Й. відносить: місце, час вчинення злочину, людей, матеріальні предмети, природнокліматичні та деякі інші фактори. Однак, ми не згодні з тим, що до обстановки скоєння злочину можна відносити людей. Найбільш підходящою буде вказівка в якості елемента на результат взаємодії людини з об'єктами, зафіксований в різних предметах матеріального і ідеального світу. Щодо шахрайства в мережі Інтернет можна також вказати і так звані віртуальні світи як підвид матеріального світу.

Таким чином, обстановку скоєння злочину складають ті об'єктивні умови, при яких воно відбувається.

Деякі дослідники характеризують час і місце скоєння злочину як окремі від обстановки самостійні елементи об'єктивної сторони складу злочину. Такий підхід цілком обґрунтований і логічний, оскільки, виходячи із загальних положень діалектики, простір, моментом якого є місце, і час є атрибути матерії. Таким чином, не існує матеріального об'єкта без просторово-часових характеристик.

Однак, на наш погляд, з точки зору криміналістики час і місце скоєння злочину необхідно розглядати як складові частини обстановки скоєння злочину. Звісно ж, що такий підхід забезпечує більш повне і цілісне розуміння як обстановку скоєння злочину, так і об'єктивну сторону в цілому.

У криміналістиці обстановка скоєння злочину розглядається як система взаємопов'язаних елементів. Наприклад, Н. В. Олиндер представляє її як систему «певним чином взаємодіючих між собою в конкретних умовах місця і часу фактів об'єктивної реальності, що обумовлюють спрямованість і хід поведінки людей в подію злочину, а також детермінують характер, механізм і умови матеріального відображення процесів, що відбуваються і явищ у вигляді характерної, щодо стійкої (для однотипних злочинів) сукупності слідів, дослідження яких дозволяє судити про сутність того, що сталося » [78, с. 13]. Однак, ми вважаємо, що таке визначення не позбавлене спірних моментів. Зокрема, незрозуміло, як і чим саме визначається взаємодія зазначених автором елементів.

Схожої позиції дотримується Панов М. І., який, зокрема, зазначає, що обстановку скоєння злочину можна визначити як «систему різного роду взаємодіючих умови місця і часу, речові та фізико-хімічні, метеорологічні умови, виробничі фактори, особливості поведінки учасників події і інші умови об'єктивної реальності, що склалися в момент події злочину і в сукупності впливають на спосіб його вчинення та механізм, що виявляється в різного роду сліди, що дозволяють судити про особливості цієї системи » [81, с. 758].

Найбільш повним і докладним представляється визначення, дане О. В. Пчеліною, згідно з яким під обстановкою вчинення злочину розуміється «обмежена просторово-часовими рамками конкретної події злочину система, що включає матеріальні, соціально-психологічні елементи навколишнього злочинця і спеціально обраної ним середовища, в якій відбувається злочинне діяння, а іноді і деяких його учасників, здатну. .. визначати характер поведінки людей, що беруть участь в ньому, обумовлювати методику його розслідування» [90, с. 118].

Можна констатувати, що єдиної думки щодо змісту поняття обстановки скоєння злочину в криміналістиці до сих пір немає. Для цілей цього дослідження найбільш підходящим є визначення обстановки скоєння злочину, дане А. В. Тарасюком: «Система взаємообумовлених елементів, в просторових межах яких відбувається взаємодія учасників злочину, а також різних інших обставин об'єктивної середовища, що склалися на певний момент розслідування і що впливають на формування слідів злочину, розкриття і розслідування злочину» [100, с. 184].

Дане визначення зручно тим, що в ньому: по-перше, обстановка розглядається саме як система; по-друге, вказується необхідний зв'язок складових елементів обстановки з діями учасників злочину; по-третє, автор вказує на те, що в поняття можуть бути включені і інші елементи (обставини об'єктивної середовища), надаючи тим самим самостійне вирішення питання про зміст поняття обстановки скоєння злочину при дослідженні будь-якого складу злочину або розслідуванні злочину.

Таким чином, можна зробити висновок, що обстановкою вчинення інтернет-шахрайства є система взаємообумовлених і взаємопов'язаних елементів, в просторових і часових межах яких відбувається взаємодія між злочинцями та їхніми жертвами, а також тих обставин об'єктивної середовища, які мали місце на момент розслідування і впливали на формування слідів злочину, його виявлення та розслідування.

Звісно ж, що часом вчинення шахрайства в мережі Інтернет є час закінчення суспільно небезпечного діяння незалежно від моменту настання

суспільно небезпечних наслідків. Конкретний час скоєння даного злочину, як, втім, і інших комп'ютерних злочинів, обчислюється періодами часу, тривалість яких залежить від різних чинників, що мають відношення до діяльності потерпілих (наприклад, графік роботи потерпілого за комп'ютером).

Характеризуючи місце скоєння інтернет-шахрайства, слід підкреслити, що на відміну від традиційних видів шахрайства, в даному випадку злочинець і потенційна жертва, з моменту початку вчинення злочину і закінчуючи моментом настання суспільно небезпечних наслідків, можуть перебувати на значній відстані один від одного.

Як вказує П. Л. Фріс, «при вчиненні злочинів у сфері комп'ютерної інформації з використанням нових телекомунікаційних технологій і засобів електрозв'язку місце вчинення суспільно небезпечного діяння, як правило, не збігається з місцем реального настання суспільно небезпечних наслідків. Таких місць може бути декілька. Вони можуть бути віддалені один від одного на значні відстані, перебувати в транспортних засобах, різних установах, на ділянках місцевості, в тому числі в різних країнах і на континентах. ... Тому місцем скоєння злочину ... найдоцільніше вважати транспортний засіб, ту ділянку місцевості або територію тієї установи, організації, держави, де було скоєно суспільно небезпечні діяння незалежно від місця настання злочинних наслідків » [103].

Звісно ж, що такий підхід до розуміння місця скоєння злочину є найбільш прийнятним, якщо мова йде про комп'ютерні злочини і, зокрема, про інтернет-шахрайство. З огляду на те, що в даний час доступ в Інтернет можна отримати майже в будь-якому місці, на наш погляд, буде необґрунтованим вважати місцем скоєння злочину місце настання суспільно небезпечних наслідків. В іншому випадку це може привести до абсурдної ситуації, коли, наприклад, суспільно небезпечні наслідки настануть у міському парку, де потерпілий, сидячи на лавці з ноутбуком, працював в Інтернеті.

Звісно ж, що іноді виникають ситуації, при яких місцем скоєння злочину може бути також і місце настання суспільно небезпечних наслідків. Однак в

таких випадках злочинець і жертва, швидше за все, віддалені один від одного незначно.

Завершуючи розгляд обстановки скоєння шахрайства в мережі Інтернет, можна зазначити таке.

1. Обстановкою здійснення інтернет-шахрайства є система взаємообумовлених і взаємопов'язаних елементів, в просторових і часових межах яких відбувається взаємодія між злочинцями та їхніми жертвами, а також тих обставин об'єктивного середовища, які мали місце на момент розслідування і впливали на формування слідів злочину, його виявлення та розслідування.

2. Часом скоєння шахрайства в мережі Інтернет є час закінчення суспільно небезпечного діяння незалежно від моменту настання суспільно небезпечних наслідків. Конкретний час здійснення цього злочину, обчислюється періодами часу, тривалість яких залежить від різних чинників, що мають відношення до діяльності потерпілих.

3. На відміну від традиційних видів шахрайства, у випадку з інтернет-шахрайством злочинець і потенційна жертва, з моменту початку вчинення злочину і закінчуючи моментом настання суспільно небезпечних наслідків, можуть перебувати на значній відстані один від одного.

Однією з ознак об'єктивної сторони складу злочину є спосіб вчинення злочину, який, як відомо, вважається факультативним. У кримінальному праві факультативні ознаки можуть виступати у різних якостях. У деяких складах, описаних в статтях КК України, ці ознаки є обов'язковими. Зокрема, в складі шахрайства спосіб вчинення злочину - обов'язкова ознака, оскільки завдяки ньому законодавець проводить розмежування шахрайства та крадіжки.

З точки зору криміналістики, як і кримінального процесу, спосіб вчинення злочину має більш важливе значення, ніж в кримінальному праві, оскільки при розслідуванні злочину слідчому необхідно встановити всі обставини, що мали місце, незалежно від того, чи має визначальне значення спосіб вчинення злочину для кваліфікації діяння. У науковій літературі зазначається, що в криміналістиці спосіб вчинення злочину «є не просто сумою або якимось

комплексом актів, а певною цілісною структурою поведінки, що представляє собою певну систему. Отже, як будь-яка система, що має певну структуру, спосіб вчинення злочину утворюється з взаємопов'язаних елементів, поведінкових актів, спрямованих на підготовку, вчинення і приховування злочину. Ці акти - дії, операції, прийоми - поєднуються в певній ієрархії і субординації як частини цілеспрямованої і вольової діяльності »[105, с. 89].

Звісно ж, що тільки після розкриття способу безпосереднього досягнення злочинної мети можна ретроспективно відновити картину того, якими діями почалося вчинення злочину, а якими - закінчилося.

На визначення способу вчинення злочину дуже часто впливає мета, яку обрав злочинець і яку він переслідує. Як вірно зазначається в науковій літературі, спосіб вчинення злочину «може бути обраний не тільки в залежності від мети злочинної діяльності, яку переслідує особа, але і в залежності від умов об'єктивної обстановки, які складаються в ході здійснення діяння» [108, с. 36].

Також необхідно відзначити, що вибір способу вчинення того чи іншого злочину впливають і деякі суб'єктивні умови.

Шахрайство в мережі Інтернет має істотні відмінності як від звичайного шахрайства, так і від шахрайства в сфері високих технологій (крім Інтернету). Відмінності ці обумовлені, в першу чергу, самим Інтернетом. Справа в тому, що Мережа в розглянутих в даній роботі зазіханнях виконує одночасно дві основні функції:

1) дає більше можливостей для підвищення і підтримки максимальної анонімності шахрая;

2) в умілих руках є дієвим інструментом, що дозволяє з великим успіхом обманювати потенційних жертв.

Також необхідно врахувати і ту обставину, що вчинені в Інтернеті дії (наприклад, угоди) втрачають ознаку територіальності. Як наслідок, врегулювання спірних питань по цих діях виявляється скрутним для будь-якої конкретної країни.

Таким чином, ймовірність викриття шахрая знижується, а якщо факт обману все-таки розкритий, то можливості притягнути винних осіб до

відповідальності виявляються досить обмеженими. Цю ситуацію можна проілюструвати наступним прикладом.

Організація здійснює продаж фото- і відеоматеріалів еротичного та / або порнографічного характеру через власний сайт в мережі Інтернет. Для доступу до матеріалів відвідувачам необхідно зареєструватися, заповнивши анкету, в зміст якої входить, у тому числі, інформація про реквізити кредитної карти. Після реєстрації жертві пропонується безкоштовний ознайомчий тур по сайту, але в процесі перегляду вмісту сайту з рахунку користувача невеликими сумами списуються грошові кошти.

Наведений приклад досить добре показує потенційні можливості інтернет-шахраїв, оскільки в даному випадку списана сума в підсумку може виявитися досить малою для того, щоб потерпілий звернув на неї увагу. А в разі, якщо жертва дізналась про обман, то довести провину зловмисників буде важко, оскільки не дивлячись на те, що мав місце факт обману користувача (безкоштовний тур виявився платним), в кінцевому рахунку, послуга з надання зображень була надана. Оскільки Інтернет надає більше можливостей зберегти власну анонімність, то шахраї цілком можуть обдурити жертву.

Даний приклад також служить хорошою ілюстрацією того, чому частина потерпілих від шахрайства не звертаються в правоохоронні органи.

В остаточному підсумку, основні особливості здійснення шахрайства в мережі Інтернет залежать від обраної зловмисником схеми, виду шахрайства, а також сфери життєдіяльності, в якій збирається діяти злочинець. Цей вибір обумовлює спосіб реалізації злочинних намірів, а також те, в якому вигляді буде отримана кінцева вигода: грошові кошти, товари, послуги або інформація.

Звісно ж, що всі види шахрайства в мережі Інтернет можна умовно об'єднати в такі групи:

1. засновані переважно на використанні електронної пошти і / або інших засобів обміну повідомленнями як основних інструментів впливу на жертву;

2. шахрайства, в схемах яких центральне місце відводиться застосуванню сайтів.

Критерієм цієї класифікації є індивідуальні переваги у виборі тактики дій шахрая, які обумовлені рівнем його спеціальної підготовки, особистих переваг, обставинами об'єктивної обстановки, а також деякими іншими обставинами. Таке розмежування пояснюється також тим, що вибір основного інструменту впливу може вплинути на кінцеву кваліфікацію дій шахрая, оскільки, наприклад, якщо для досягнення кінцевого результату (заволодіння чужим майном) були використані будь-які шкідливі програми (троянські коні, віруси і т.д.), то кваліфікуватися таке шахрайство повинно за сукупністю зі статтею 361-1 КК України (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут).

Слід зазначити, що такий розподіл є умовним, оскільки на сьогоднішній день нечасто зустрічаються шахрайські схеми, в яких злочинці використовують тільки щось одне. Як приклад можна вказати деякі шахрайські схеми, в основі яких лежить клонування сайту, що належить будь-якій організації. В цьому випадку зловмисник створює якомога точнішу копію сайту- оригіналу (аж до співзвучної інтернет-адреси), проте вказує інші реквізити для розрахунків. Тут шахрай працює, як правило, тільки з сайтом. У більшості інших випадків реалізація тієї чи іншої схеми шахрайства на увазі активне використання всіх можливих електронних ресурсів. Звісно ж, проте, що така діяльність пов'язана з великим ризиком викриття, оскільки залишиться більше слідів.

Розглянемо кожну з представлених груп детальніше.

Злочини, в яких посягання на об'єкт здійснюється переважно за допомогою електронної пошти та / або інших засобів обміну повідомленнями. В цю групу входять ті види шахрайства, в яких основним інструментом реалізації злочинного задуму є служби обміну повідомленнями (Instant Messaging Service, IMS). Вхідні в цю групу злочини характеризуються тим, що майже вся робота з жертвою проходить у формі листування, а в деяких випадках для успішного для шахрая результату може вистачити одного єдиного листа.

Незалежно від того, який спосіб обміну повідомленнями обраний, в переважній більшості випадків головне, на чому акцентує увагу шахрай, це

масова розсилка певних повідомлень - спам. Така підвищена увага пояснюється тим, що метою спаму служить привернення уваги якомога більшої кількості потенційних жертв. Це особливо актуально в тих випадках, коли спам є частиною підготовчого етапу до злочину і спрямований на збір особистої фінансової та іншої конфіденційної інформації про жертви шляхом таємного впровадження на їх комп'ютери шкідливого програмного забезпечення (наприклад, програм-шпигунів), а також іншими способами, наприклад , шляхом розсилки листів з пропозицією заповнити анкету. Тому при плануванні злочину особлива увага звертається не тільки на кількість розісланих повідомлень, а й на якість їх складання.

Звісно ж, що повідомлення, що розсилається зловмисником, має відповідати трьом основним параметрам:

1) відносно невеликий розмір;

2) максимальна переконливість (ситуація дещо полегшується в тих випадках, коли жертва отримує повідомлення від людини, що знаходиться в списку друзів, що актуально для шахрайства в соціальних мережах);

3) забезпечення якомога меншу ймовірність розкриття обману і власного виявлення.

Найбільш відомим видом шахрайства в Інтернеті, який використовує можливості електронної пошти, прийнято вважати так звані «нігерійські листи». Незважаючи на те, що даний вид обману експлуатувався задовго до появи інтернет-шахрайства як такого, він до цих пір безвідмовно працює. Основний сенс «нігерійських листів» полягає в наступному.

Жертва (одна з багатьох, оскільки здійснюється масова розсилка спаму) отримує електронний лист, як правило, написане на англійській мові, від імені багатого нігерійського підданого з історією про нестабільну обстановку в його країні, результатом чого з'явилися деякі фінансові проблеми. За допомогу у вирішенні цих проблем (що полягають у виведенні коштів нігерійця в іншу країну) адресант пропонує значну суму грошових коштів. Єдине, що потрібно від одержувача листа, - вказати реквізити свого банківського рахунку для переказу всіх засобів нігерійця (після чого частина коштів буде переведена на

інший рахунок, а частина - залишиться в якості винагороди). Після того як жертва виконує прохання адресанта, відбувається зворотна ситуація, з рахунку обманутого особи списуються грошові кошти. Слід зазначити, що це не єдина тема, яку шахраї застосовують при розсилці листів. Останнім часом зустрічаються листи, що містять інформацію про, нібито, готовність перерахувати значну суму грошей від Організації Об'єднаних Націй.

Звісно ж необхідно окремо розглянути шахрайство в соціальних мережах. Даний вид обману отримав в останні роки велике поширення. Як і в інших випадках, спочатку застосовувалася стандартна тактика розсилки спаму (створення великої кількості облікових записів з подальшою розсилкою з них повідомлень якомога більшій кількості інших користувачів), однак вона швидко показала свою малоефективність. Тому через деякий час з'явився якісно новий спосіб обману користувачів соціальних мереж. Він полягав у зломі і отриманні короткочасного повного доступу до облікових записів користувачів і розсилці особливого тексту повідомлення від їх імені особам, які перебувають у списку друзів у «зламаного» користувача.

Особливістю такого способу шахрайства є те, що користувач як і раніше має можливість користуватися своїм обліковим записом, тому потенційні жертви з більшою ймовірністю надійдуть так, як того бажає шахрай (наприклад, завантажити за вказаною в повідомленні посиланням програму і встановити її на свій комп'ютер. Програма виявиться шкідливою).

В даний час аналогічний метод розсилки повідомлень застосовується і з використанням сервісів миттєвого обміну повідомленнями. У разі досягнення успішного результату на комп'ютер жертви, в більшості випадків, встановлюється шкідливе програмне забезпечення, призначення якого - крадіжка особистої інформації, наприклад, даних кредитних карт[102].

Дуже часті випадки, коли своєчасне виявлення подібних програм неможливо за допомогою спеціальних засобів, оскільки компанії-виробники антивірусних та інших захисних програм не завжди встигають вчасно реєструвати нові шкідливі програми. Звісно ж, що в таких випадках безпека комп'ютера користувача і наявної на ньому інформації буде багато в чому

залежати від комп'ютерної грамотності цього користувача, тобто володіння достатнім обсягом інформації про роботу в Інтернеті і вміння користуватися цими знаннями.

Злочини, в яких посягання на об'єкт здійснюється переважно з використанням можливостей інтернет-сайтів. Данную групу становить більшість посягань, відмінна риса яких - використання сайтів як основного інструменту впливу. На наш погляд, серед напрямків діяльності шахраїв з даної групи основними будуть наступні:

1) інвестиційні схеми;

2) заробіток;

3) «чарівні гаманці»;

4) аукціони і інтернет-торгівля;

5) кардинг;

6) онлайн-казино і лотереї;

7) клонування сайтів.

Звісно ж, що найбільшу небезпеку на сьогоднішній день представляють інтернет-торгівля (рідше, аукціони), кардинг, лотереї і клонування сайтів. Розглянемо деякі із зазначених видів шахрайства докладніше.

Діяльність аукціонів і інтернет-магазинів має досить багато спільного, а саме: товар, який потенційний покупець має намір придбати, або взагалі не надсилається, або приходить посилка, але її вміст зовсім інший; плату за означений товар просять перерахувати до того, як бажана річ дійде до одержувача.

Можна виділити два основних способи, які застосовуються шахраями на аукціонах:

1) повідомлення учасників аукціону, які не змогли придбати бажаний предмет, про те, що покупець відмовився від покупки і їм надається «другий шанс». У повідомленні дається адреса сайту, де пропонується здійснити приватну угоду. Однак, вислявши необхідну суму, жертва нічого не отримує;

2) повідомлення учасників про необхідність підтвердження платіжних реквізитів. Посилання, по якій потерпілий проходить, веде на підроблений сайт, таким чином, він несвідомо передає важливу інформацію злочинцям.

На відміну від аукціонних, шахраї, що спеціалізуються на роздрібній торгівлі онлайн, мають у своєму розпорядженні більш різноманітний арсенал для досягнення поставлених цілей. Основними способами обману є наступні:

1. Створення інтернет-магазину, в якому на заявлені товари встановлюються занижені ціни для залучення якомога більшої кількості покупців. Однак після оплати покупки клієнтові нічого не висилається. 2. Встановлення так званих плаваючих цінників, при якій, під час знаходження потенційного клієнта на сайті магазина, ціни на товари трохи збільшуються. В даному випадку відвідувач сайту, бачачи зміну ціни на товар, що цікавить, проте, погоджується на покупку. Така поведінка пояснюється тим, що дуже багато потерпілих від дій шахраїв, найчастіше, до останнього моменту або взагалі не помічають підозрілих речей, або трактують їх на користь злочинців. Підвищення ціни також може бути витлумачено покупцем як планована зміна з боку адміністрації магазину.

3. Прихована диференціація клієнтів магазину в залежності від їх матеріального становища. Даний спосіб шахрайства використовують, в основному, ті компанії, які ведуть докладний облік своїх клієнтів (наприклад, туроператори). Коли після авторизації на сайті магазину або компанії система розпізнає більш платоспроможних покупців, відбувається непомітне для цих клієнтів збільшення цін на товари або послуги, в той час як для інших вони залишаються на колишньому рівні.

Одним з найбільш поширених видів інтернет-шахрайства було і залишається шахрайство з кредитними картами - кардинг.

Поняттям «кардинг» прийнято позначати рід шахрайства, при якому проводиться операція з використанням банківської карти або її реквізитів, що не ініційована або не підтверджена її власником. Реквізити платіжних карт злочинці, як правило, отримують зі зламаних серверів інтернет-магазинів, платіжних та розрахункових систем (WebMoney, PayPal та ін.), а також з

персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, шляхом впровадження шкідливого програмного забезпечення) .

Кардінг має безліч схем, які передбачають найрізноманітнішу реалізацію. У будь-якому випадку шахрайство з кредитними картами можна вважати злочином у сфері високих технологій, оскільки воно може мати форму і звичайного шахрайства, і злочини в мережі Інтернет, і змішаного, коли, наприклад, в організованій злочинній групі частина спільників працює через Інтернет (спам, крадіжка інформації і т.д.), а інша частина здійснює кримінальну діяльність в реальному світі (створення фальшивих кредитних карт на основі здобутої інформації, переведення в готівку грошових коштів через банкомати, організація і підтримання роботи фіктивних ca11-центрів і т.д.). Як приклад розглянемо одну зі схем шахрайства з кредитними картами в мережі Інтернет.

Створюється фіктивний інтернет-сайт, що пропонує послуги з продажу товарів (наприклад, електронної техніки з Китаю). Умовою придбання товарів зазначаються тільки безготівкова оплата. У зв'язку з цим відвідувачам сайту пропонується зареєструватися, надавши тим самим деяку особисту інформацію.

Після реєстрації і вибору товару, що цікавить жертва оформляє замовлення, вказуючи реквізити своєї кредитної картки, необхідні для оплати. Тут важливо відзначити, що злочинці можуть попросити вказати всі реквізити кредитної карти (наприклад, щоб потім створити клон кредитної картки і зняти з неї всі залишилися грошові кошти). Це може подіяти на неуважних або недосвідчених користувачів. Далі, з рахунку жертви знімаються кошти на оплату і доставку товару, після чого приходить повідомлення про те, що обраний товар через певний період часу буде доставлений. Однак, в кінцевому рахунку, жертва нічого не отримує. До того ж у шахраїв буде вся необхідна інформація для того, щоб спустошити рахунок покупця, а потім сховатися.

Дану схему можна назвати класичною в силу її поширеності. Відзначимо також, що можливі варіанти, коли жертва отримує своє замовлення, проте це буде або не той товар, який був замовлений спочатку, або той, але бракований або з іншими недоліками. Також можна відзначити, що представлена схема -

яскравий приклад того, наскільки органічно можуть поєднувати різні шахрайські схеми.

У сучасних умовах в Україні досить поширеним способом обману є «гра» на бажанні заробити. Реалізація такого напряму може бути надзвичайно різноманітною. Як приклад реалізації даного способу можна навести таку загальну схему.

Створюється сайт, що пропонує високий заробіток за передрук відсканованих книг для будь-якої відомої бібліотеки. Процес роботи з текстами описується таким чином, щоб потенційна жертва мала якомога менше сумнівів з приводу сумлінності пропозиції. Для досягнення цієї мети можна використовувати спеціальної лексики, яка, в кінцевому рахунку, може не нести будь-якої змістового навантаження, однак, ускладнюючи своєю присутністю текст, здатна ввести потенційну жертву в оману. Єдиною умовою, яку необхідно виконати перед початком роботи, - перерахувати певну грошову суму в рахунок поштових витрат, які, в свою чергу, пов'язані з майбутньою трудовою діяльністю. Після того як достатня кількість людей попалося в цю пастку, шахраї стирають всі сліди своєї діяльності і зникають.

З огляду на те, що жертви перераховують відносно невеликі суми на рахунок шахраїв, розслідування такого злочину може бути ускладнений великою кількістю потерпілих, що не стануть звертатися за допомогою до правоохоронних органів, вважаючи, що їм буде в цьому відмовлено з причини малої суми заподіяної шкоди (хоча, на насправді, з цього приводу могли вже звернутися велика кількість потерпілих і кримінальне провадження порушили). Причиною незвернення може бути також небажання самого потерпілого / потерпілих зв'язуватися з правоохоронними органами через малу суму втрачених коштів. Як можна помітити, описаний вище приклад має деяку схожість з «нігерійськими листами».

Звісно ж необхідним відзначити і такий різновид інтернет-шахрайства, як фішинг. На сьогоднішній день він є найбільш поширеним методом крадіжки номерів платіжних карт і полягає в створенні шахраями сайту, який буде

користуватися довірою у користувача, наприклад - сайт, схожий на сайт банку, через який і крадуться реквізити платіжних карт.

Фішинг як різновид шахрайства має таку особливість, а саме: може бути реалізований за допомогою сервісів обміну повідомленнями, сайтів, засобів стільникового або телефонного зв'язку, причому як окремо, так і в комбінації [98] .

Фішинг, як один з видів шахрайства, характеризується, в першу чергу, прагненням отримати ідентифікаційні дані для подальшого розкрадання грошових коштів в якості основної мети діяльності (наприклад, реквізитів банківських рахунків або кредитних карт). При фішингу також використовуються розсилки. Відмінні риси таких розсилок наступні:

1) повідомлення надсилаються, як правило, від відомого імені (наприклад, від імені банку або платіжної системи);

2) дуже часто лист містить посилання на сайт, який або є точною копією оригіналу, або перенаправляє користувача на потрібну злочинцю сторінку. Мета даного сайту - «вивудити» (звідси і назва терміна «фішинг» - англ, phishing від fishing - вивудження) необхідну конфіденційну інформацію з жертви.

Іноді замість розсилок злочинці застосовують метод прозвону. Даний метод застосовується в тих випадках, коли шахраї отримують базу даних власників кредитних карт після злому локальної мережі банку або, як варіант, отримання цієї інформації від спільника, який працює в цьому банку. Суть методу полягає в тому, що клієнтам банку дзвонить робот і від імені банку повідомляє, наприклад, про факти несанкціонованого використання їх кредитної картки і подальшої необхідності передзвонити за наданим номером для вказівки PIN-коду карти з метою її блокування [10,с. 102].

Клонування сайтів як підвид мережевого шахрайства найчастіше зустрічається в комбінованих схемах обману, коли поряд з Інтернетом шахраї активно використовують стільниковий зв'язок. Такі схеми ефективні при проведенні фіктивних лотерей, коли на телефон жертви приходить SMS з повідомленням про виграш цінного призу (наприклад, автомобіля) на основі

випадання чисел, що становлять номер телефону потенційної жертви. У повідомленні також вказується адреса сайту компанії, що надала приз (за цією адресою розташований клон), де жертва зможе дізнатися про умови отримання призу. Після цього роль стільникового зв'язку зводиться до мінімуму.

Інформація, що міститься на сайті-клоні інструкція вказує на необхідність перерахування деяких сум грошових коштів на різні цілі. Наприклад, якщо мова йде про автомобіль як приз, то приводом до перерахування грошей може бути страховка, транспортування автомобіля і так далі до тих пір, поки жертва не відмовиться перераховувати нові суми на рахунку зловмисників.

Клонування сайтів досить часто зустрічається і в формі благодійних фондів. У таких випадках зловмисники створюють якомога точнішу копію певного інтернет-сайту фонду зі збору коштів на благодійні потреби (наприклад, проведення дорогої операції і подальшого курсу лікування за кордоном для певної людини), реєструючи підробку за адресом, співзвучним з оригінальним. При цьому платіжні реквізити, природно, вказуються інші.

Цікавою особливістю даного шахрайства є те, що сайти-клони ведуть більш активну роботу, ніж оригінали, зокрема, виробляючи масові розсилки по електронній пошті листів з проханням про пожертвування (чим не займаються легальні організації подібного типу) [11, с. 197]. У деяких випадках, зловмисники можуть публікувати новини на сайті - клоні, найчастіше вигадані, про стан здоров'я особи, на користь якої збираються кошти. Останні покликані викликати почуття жалості у читачів і, тим самим, спонукати їх зробити пожертвування.

Слід врахувати, що шахраї можуть зареєструвати сайт-клон в доменній зоні іншої держави, тому мова йде про серйозний злочин, розслідування якого може ускладнитися необхідністю взаємодії із зарубіжними правоохоронними органами.

Звісно ж, що незабаром велике поширення отримає так зване шахрайство в онлайн-іграх. В останні 3-5 років все більшої популярності набувають масові багатокористувацькі онлайн-ігри, в яких тисячі користувачів Інтернету мають можливість спільно проводити дозвілля. За ці роки аудиторія даного виду

розваг істотно зросла, як і кількість представлених розробниками ігор. У зв'язку з цим також істотно зросла активність шахраїв і розробників шкідливого програмного забезпечення.

Ігровий процес переважної більшості онлайн-ігор побудований таким чином, що гравцеві необхідно провести досить багато часу в грі і докласти багато зусиль для досягнення певного успіху, що виражається у вигляді високого ступеня розвитку ігрового персонажа, наявності високорівневих ігрових предметів і великої кількості ігрової валюти [13, с. 18]. Тому, з огляду на те, що вік ігровий аудиторії практично не має обмежень, логічним буде висновок про те, що є категорія людей, які не мають надто багато вільного часу, проте мають достатній заробіток. Дана категорія і становить коло потенційних жертв шахрайства в онлайн-іграх. Оскільки є люди, готові заплатити за ігрові цінності реальні гроші, завжди знайдуться ті, хто готовий запропонувати ці цінності.

Фахівці Лабораторії Касперського вказують, що є кілька основних методів для крадіжки ігрової конфіденційної інформації, яку згодом можна використовувати в шахрайських цілях:

1. Використання соціальної інженерії в формі фішингових повідомлень.

2. Використання програмних вразливостей ігрових серверів з метою отримання несанкціонованого доступу до баз даних користувачів, що дозволяє викрасти паролі від облікових записів гравців.

3. Використання шкідливих програм [15, с.57].

Серед різних способів здійснення шахрайства можна виділити наступні способи, які застосовуються до шахрайства в онлайн-іграх (а також деяких інших видів шахрайства в мережі Інтернет):

1. Фішинг.

2. Створення фіктивних інтернет-магазинів, які здійснюють торгівлю ігровими цінностями.

3. Обман і зловживання довірою всередині ігрового світу, результатом чого буде незаконне безоплатне вилучення грошових коштів на користь зловмисника.

4. Спам, поєднаний з поширенням шкідливих програм. Звісно ж необхідним зазначити, що в національній правовій науці проблеми взаємодії реальної і віртуальних економік (в тому числі і економік ігрових світів) не вивчені. Тому дослідження шахрайства в онлайн-іграх, як вид інтернет-шахрайства, поки що можливо лише на теоретичному рівні.

Розглядаючи проблему підробок електронних грошей, необхідно зазначити наступне:

Незважаючи на те, що електронні гроші активно використовуються як фізичними, так і юридичними особами до недавнього часу законодавством України термін «електронні гроші» взагалі не передбачався. Лише у 2013 р. були внесені зміни у Закон України «Про платіжні системи та переказ коштів в Україні» і у ст. 15 цього Закону «електронні гроші» законодавець визначили як одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу іншими особами, ніж особа, яка їх випускає, і є грошовим зобов'язанням цієї особи, що виконується в готівковій або безготівковій формі. Випуск електронних грошей може здійснювати виключно банк, який і бере на себе зобов'язання з їх погашення. Недостатня нормативна урегульованість питань пов'язаних із створенням, введенням/виведенням коштів, ліквідацією електронних гаманців полегшує використання їх у злочинній діяльності. Основні властивості віртуальних гаманців, якими зловживають злочинці, полягають у можливості:

− швидкого, дешевого проведення трансакцій і легкості обходу обмежень, зокрема за сумами платежів;

− організації та проведення нелегальної діяльності за допомогою мережі Інтернет (шахрайство, хакерство, порноіндустрія, торгівля зброєю і наркотиками тощо), доходи від якої надходять за допомогою платежів в електронних грошах; − ухилення від сплати податків;

− приховування слідів трансакції (послідовного ряду трансакцій);

− використання третіх осіб; − де-персоніфікованого введення/виведення готівки; − «обходу» банківської системи, яку жорстко регулюють з питань легалізації коштів, отриманих злочинним шляхом [25, с. 275].

Можна виділити чинники, які погіршують ефективність боротьби зі злочинами у цій сфері. До них належать: − недосконаліть національного законодавства; − труднощі при отриманні доказової бази; − транснаціональний характер злочинної діяльності; − недосконаліть процедури міжнародного співробітництва та ін.

Для того аби продемонструвати конкретні приклади підробки електронних грошей, нагадаємо резонансну справу, коли правоохоронці виявили на території ДП "Лікувально-оздоровчий" ІЕЗ ім. Патона" 200 одиниць комп'ютерного обладнання для генерації криптовалюти Bitcoin, які працювали з порушенням законодавства.

У постанові суду №759/11642/17 від 4 серпня 2017 року йдеться, що в ході досудового розслідування встановлено, що кілька осіб за попередньою змовою, переслідуючи особисту корисливу зацікавленість, вирішили здійснити підробку банківських документів. Слідчі відзначали, що випуск і обіг «грошових сурогатів» криптовалюти Bitcoin на території України заборонені згідно ч. 2 ст. 32 Закону України "Про Національний банк України". У документі також наголошулося, що ці процеси порушують вимоги Законів України "Про Національний банк України", "Про банки і банківську діяльність", статті 9 Закону України "Про платіжні системи та переказ коштів в Україні", згідно з якою платіжні організації платіжних систем, учасники платіжних систем та оператори послуг платіжної інфраструктури мають право здійснювати діяльність в Україні тільки після їх реєстрації шляхом внесення відомостей про них до Реєстру.

Слідчий зазначив, що для реалізації злочинного наміру в непрацюючому басейні ЛВЦ були розміщені 200 одиниць комп'ютерного обладнання, так звані, "Майнери". При цьому ніяких договорів не було укладено, так як за згаданою вище групою сприяли посадові особи Лікувально-відновлювального центру.

Отож, як бачимо, і надалі отримана криптовалюта використовується як засіб платежу шляхом здійснення обмінних операцій на електронні гроші офіційних платіжних систем, шляхом підробки електронних платіжних доручень та інших банківських документів. Суд дозволив Нацполіції провести

огляд за адресою басейну "Лікувально-відновлювального центру ІЕЗ ім. Патона" з метою розшуку і вилучення речей та документів, пов'язаних з генерацією Bitcoin. На разі за даним провадженням остаточного рішення суду немає.

1.3. Характеристика особистості типового злочинця

Для проведення найбільш повного аналізу особистості типового інтернет-шахрая представляється необхідним розглядати дане питання в більшій мірі з кримінологічної точки зору, оскільки саме в рамках кримінології вчення про особу злочинця отримало найбільший розвиток.

У кримінологічної літературі зазначається, що вивчення особистості злочинця передбачає розкриття структури цієї особистості, що представляє собою впорядковане співвідношення властивостей (ознак), що характеризують порушника правової заборони. Дана структура включає в себе шість груп ознак:

1) соціально-демографічні ознаки (стать, етнічна приналежність, вік і ін.);

2) соціальні ознаки, які проявляються в різних сферах життєдіяльності (наприклад, професія або сімейний стан);

3) моральні ознаки (відношення до релігії та ін.);

4) кримінально-правові ознаки (наявність судимості та ін.);

5) фізичні ознаки (наявність захворювань і ін.);

6) психологічні ознаки [41, с. 302].

Взаємодія властивостей (ознак) особи, що скоює злочин і обстановки вчинення посягання знаходить своїй зовнішній прояв в конкретній злочинній поведінці.

Однією з характерних особливостей, властивих кіберзлочинності, є переважання злочинців чоловічої статі. Незважаючи на те, що серед користувачів Інтернету співвідношення жінок і чоловіків приблизно однаково, останні виявляють більш високу кримінальну активність. Переважання осіб чоловічої статі серед інтернет-злочинців, як і в більшості традиційних злочинів,

пояснюється історично сформованим більш високим рівнем соціальної активності чоловіків.

Аналізуючи вік різних інтернет-злочинців, можна відзначити, що переважна більшість порушених посягань відбувається особами у віці до 34 років, причому пік припадає на період приблизно з 18 до 25 років. Як приклад, що підтверджує наведені цифри, можна вказати результати, отримані І. І. Кісілюк. Вивчивши особистості 111 злочинців, розподілила їх за такими віковими категоріями:

1) до 18 років - 14 осіб (12,6%);

2) 18-24 років - 73 людини (65,8%);

3) 25-34 року - 16 осіб (14,4%);

4) 35-44 року - 5 осіб (4,5%);

5) 45-54 роки - 1 людина (0,9%);

6) 55 і старше - 2 людини (1,8%) 32 [44, с. 286].

Вона вказує, що, основна частина злочинців - студенти коледжів і вузів. Всього ж частка учнів всіх рівнів склала приблизно 47%, що еквівалентно 26-28% від усієї аудиторії Інтернету (за соціальним станом). Таким чином, саме учні та студенти вузів виявляють в Інтернеті підвищену кримінальну активність. Одним з пояснень такого стану речей є те, що вік від 20 до 40 років вважається періодом найвищої активності у більшості людей.

Звісно ж, що більш низький середній вік інтернет- шахраїв, як і інших мережевих злочинців, свідчить про поступове омолодження частини злочинності взагалі. На наш погляд, існує реальна загроза переходу більшої частини традиційних корисливих злочинів в категорію злочинів у сфері високих технологій, частина яких становлять також інтернет-злочини.

Фахівці з вищою освітою становлять приблизно 35% від загального числа злочинців. Близько 33% суб'єктів мали постійне місце роботи, деякі з них поєднували роботу і навчання, 21,4% на момент вчинення злочинів не вчилися і не працювали, перебуваючи на утриманні батьків або інших родичів. Відзначимо, що традиційні шахраї, в порівнянні з інтернет-злочинцями, в більшій кількості випадків не мають постійного місця роботи. Частково це

пояснюється високим відсотком рецидиву (відбувши покарання, шахраї часто з різних причин не знаходять роботу, відразу починаючи займатися злочинною діяльністю).

Отже, близько 70% злочинців не мали постійних джерел доходу, що пояснює причину великої частки корисливих посягань серед загальної кількості злочинів, скоєних в мережі Інтернет.

Необхідно відзначити один недолік щодо інформації про місце роботи і джерела доходу. І. І. Кісілюк не вказала інформацію про тих злочинців, які працювали безпосередньо в Інтернеті. Справа в тому, що більшість інтернет-злочинців, так чи інакше, мають певний набір спеціальних знань. В Інтернеті є багато можливостей заробітку, в тому числі і за допомогою застосування таких знань. Пропозиції можуть носити як легальний (створення інтернет-сайтів, настройка поштових серверів і т.д.), так і нелегальний характер (наприклад, написання шкідливих програм для вирішення конкретних завдань). Таким чином, з'ясувавши, яким саме способом злочинець заробляв на життя, можна отримати також і інформацію про осіб, з якими він взаємодіяв, і, отже, з'явиться більше шансів встановити всіх членів злочинної групи.

Близько 35% інтернет-злочинців мають середню спеціальну освіту, тобто закінчили школу, коледж, або вчилися на 1-2 курсах інститутів. Приблизно така ж кількість мають незакінчену вищу освіту (в основному, студенти старших курсів вищих навчальних закладів). Лише близько 23% злочинців мають вищу освіту. Примітним є те, що близько двох третин з усіх інтернет-злочинців мають вищу або незакінчену вищу технічну освіту, і лише близько 33% - середню або середню спеціальну [44, с. 287].

Однією з характерних особливостей кіберзлочинності взагалі і інтернет-шахрайства, зокрема, є відсутність судимості (або вчинення злочину вперше) у злочинців - близько 90% всіх випадків. Дійсно, якщо порівнювати шахрайство в мережі Інтернет і звичайне шахрайство, то можна побачити, по суті, дві протилежні картини. Однак видається, що така тенденція, з часом, піде на спад. У порівнянні з традиційними видами шахрайства інтернет-шахрайство є досить

молодим видом злочину. Тому прояв подібної кримінальної активності в мережі Інтернет в даний час являє собою свого роду «пробу пера».

Згодом будуть з'являтися нові, більш ефективні можливості для здійснення злочинних посягань. Це, в свою чергу, може спонукати до здійснення злочинів і тих осіб, які в минулому їх здійснювали і понесли за це покарання. Оскільки відбувши термін, шахрай може отримати інформацію про нові або більш вдалі варіанти реалізації старих способів скоєння злочину, він цілком може піти на вчинення нового злочину. Ситуація ускладнюється, в тому числі, погано розвиненою системою реабілітації осіб, залучених до кримінальної відповідальності.

Аналіз морально-правових характеристик особистості інтернет- злочинців, представлені в роботах різних дослідників, показує, що підслідні, так чи інакше, визнавали свою провину повністю або частково.

Звісно ж, що подібна поведінка складається в результаті взаємодії таких обставин:

1) страх перед правоохоронними органами, частково пов'язаний з відсутністю досвіду спілкування з ними (як було зазначено вище, практично всі засуджені вчиняли злочин вперше);

2) сліди дуже багатьох інтернет-злочинів взагалі і шахрайств, зокрема, погано приховані, як наслідок, доказ провини частково полегшено. Тому затримані, розуміючи, що заплутати слідство або іншими способами зняти з себе звинувачення вони не в змозі, погоджуються на співпрацю.

У зв'язку з цим ми вважаємо, що подібний підхід повинен отримати розвиток - необхідно використовувати всі законні засоби для того, щоб злочинці самі приходили до висновку про необхідність співпраці зі слідством, так як тільки в цьому випадку можна отримати максимальну кількість інформації і, відповідно, забезпечити найбільш повне і об'єктивне розслідування вчиненого діяння.

Останнє, на що необхідно звернути увагу - в основному, позитивні характеристики за місцем роботи та місцем проживання. Дуже рідкісні випадки, коли характеристики формальні і майже ніколи - негативні. На додаток до

цього можна відзначити, що практично ніхто з обвинувачених ніде на обліках не перебував.

Існує також певний набір особливостей особистості, які обумовлюють вибір конкретної злочинної діяльності, яку шахрай збирається здійснювати.

Серед різних поглядів на характерні ознаки особистості типового шахрая найбільш придатною для цілей цього дослідження представляється позиція І. І. Котюка та П. Д. Біленчука, які, серед інших соціально-психологічних ознак особистості, вказують наступні:

1. Глибокі пізнання в різних сферах людської діяльності.

2. Визначальний мотив злочину - користь. Співвідносячи дану характеристику з зразковим віком типового інтернет- шахрая (приблизно 18-35 років, причому основний відсоток припадатиме на період з 18 до 25 років), можна зробити висновок, що типовий інтернет-шахрай - студент вузу або установи середньої професійної освіти, не працюючий і, можливо, знаходиться на утриманні батьків або інших родичів.

3. Хороші комунікативні якості, винахідливість, спостережливість. У практиці розслідування шахрайств в мережі Інтернет відомі випадки, коли злочинці успішно спілкувалися зі своїми жертвами від імені жінок, будучи при цьому чоловіками (такі випадки зустрічаються, в основному, в шлюбних аферах з використанням сайтів знайомств).

4. Дуже багато шахраїв не перебувають у шлюбі і не мають дітей. Даний список можна доповнити наступними ознаками, характеризують інтернет-шахраїв: по-перше, пізнання в сфері інформаційних технологій, рівень яких багато в чому визначає вид і спосіб шахрайства; по-друге, багато інтернет-шахраї, так чи інакше, мають відношення до ІТ-сфери, наприклад, є програмістами, працюють системними адміністраторами і т.д., хоча і зустрічаються особи, які не є кваліфікованими фахівцями в сфері ІТ [56, с. 65]. Таким чином, при розслідуванні конкретних злочинів коло можливих суб'єктів можна істотно звузити.

Від характерних особливостей особистості типового інтернет-шахрая багато в чому залежить той вид шахрайства, на якому він спеціалізується.

Слід зазначити, що інтернет-шахрай планує саме незаконну діяльність і саме в Інтернеті, керуючись, в більшості випадків, міркуваннями раціональності, а не рівнем своїх знань в сфері інформаційних технологій або прихильності до комп'ютерів, що більш властиво таким злочинам, як неправомірний доступ до комп'ютерної інформації, створення, використання і поширення шкідливих програм для ЕОМ тощо.

У деяких випадках однією з важливих якостей особистості інтернет-шахрая є наявність організаторських здібностей. Справа в тому, що деякі види інтернет-шахрайства є технічно складними в плані виконання, тому в їх вчиненні беруть участь кілька людей. У такій ситуації запорукою успішної реалізації поставленого завдання будуть чітко розподілені ролі і постійний контроль. Розподіл ролей в групі обумовлює також відмінність набору особистісних якостей кожного її члена. Прикладом такого поділу можна вважати шахрайство в шлюбної сфері. При скоєнні даного злочину групою, очевидно, що, наприклад, комунікативні якості важливіші безпосереднім виконавцям (це особи, які безпосередньо займаються листуванням з жертвами), ніж організатору.

1.4. Загальна характеристика кола потерпілих від економічних злочинів, що вчиняються в кіберпросторі

Згідно зі статтею 55 КПК України, «Потерпілим у кримінальному провадженні може бути фізична особа, якій кримінальним правопорушенням завдано моральної, фізичної або майнової шкоди, а також юридична особа, якій кримінальним правопорушенням завдано майнової шкоди» [61]. Таким чином, всі потерпілі від злочинів поділяються на дві групи: фізичні особи та юридичні особи. З огляду на те, що інтернет-шахрайство носить корисливий характер, можна виділити наступні підгрупи потерпілих:

1) фізичні особи, в тому числі іноземні;

2) підприємства зв'язку і провайдери мережі Інтернет;

3) банки та інші кредитні організації;

4) магазини електронної торгівлі;

5) інші комерційні і некомерційні організації;

6) інші іноземні юридичні особи.

Розглянемо докладніше деякі з представлених груп, що найчастіше зустрічаються при розслідуванні інтернет-шахрайства.

Фізичні особи формують найбільшу групу потерпілих, яка за різними оцінками складає близько 20-25% всіх злочинів в мережі Інтернет, а у випадках з шахрайством ця група, разом з іноземними фізичними особами, становить основну масу потерпілих (понад 80% від загального числа) [50].

У більшості випадків (приблизно 75%) потерпілі поводяться віктимно, внаслідок чого злочин стає можливим. Причинами цього можуть бути простодушність і довірливість або корисливі мотиви, тобто бажання максимально збагатитися при мінімальних витратах і зусиллях. До названих причин можна додати також безпечність, неуважність (в тому числі до попереджень платіжних систем, банків, різних сервісів і т.д.) і комп'ютерну безграмотність, оскільки досить велика кількість користувачів мережі Інтернет не робить жодних було заходів щодо захисту свого комп'ютера і особистої конфіденційної інформації від різних загроз (наприклад, іншого шкідливого, в тому числі шпигунського програмного забезпечення). Результатом цього є істотне полегшення роботи шахраїв. Звісно ж, також, що віктимна поведінка є одним з головних факторів незахищеності конфіденційної інформації потенційної жертви.

Розглянемо віктимну поведінка фізичних осіб як потенційних жертв злочину з точки зору шахрайства в мережі Інтернет. Під віктимною поведінкою розуміється схильність суб'єкта до такої поведінки, при якому шанси на вчинення злочину щодо цього суб'єкта вище, ніж в тому випадку, коли він поводиться належним чином. Причому діяння цього суб'єкта, виражені в формі дії або бездіяльності, не мають на увазі прямого наміру зробити можливим вчинення злочину. Тут, в більшості випадків, має місце легковажне або недбале ставлення до питань безпеки [54, с. 102].

Таким чином, віктимною слід визнавати таку поведінку (що викликає, протиправне, легковажне, недбале, аморальне), яке, в кінцевому рахунку, послужило приводом для вчинення злочину. Щодо інтернет-злочинів віктимна поведінка проявляється, як правило, в легковажності і недбалості. Це виражається, зокрема, в недотриманні правил безпеки і відмову слідувати різним рекомендаціям, які належать, наприклад, до роботи з платіжними системами або до зберігання інформації в пам'яті комп'ютера. Передумовами віктимної поведінки є такі: 1) відсутність необхідних знань і умінь користування комп'ютером, їх мережею, програмним забезпеченням; 2) недбале ставлення до конфіденційної інформації або легковажний розрахунок на те, що нічого не станеться. Звісно ж необхідним вказати ще одну передумову, яку можна віднести до обох пунктів, - неправильні уявлення користувача про ступінь захищеності інформації [63, с.10]. В даному випадку проблема полягає в тому, що набір програмного забезпечення у більшості користувачів якщо не однаковий, то дуже схожий. Популяризація різних програм завжди викликає інтерес у створювачів вірусів, оскільки в таких випадках одна шкідлива програма зможе бути успішно застосована відносно більшої кількості користувачів. Навіть використання захисних програм (антивірусів, фаєрволів і т.д.) не здатна забезпечити стовідсотковий захист інформації.

Таким чином, в незалежності від того, про який вид шахрайства в Інтернеті йде мова, характеристика кола потерпілих осіб, багато в чому, схожа. Більшість жертв інтернет-шахраїв є людьми, слабо знайомими з технікою безпеки при роботі в Мережі. Тому вони не в змозі оцінити ситуацію, причому деяким з цих жертв (відносно невелика група людей) властиво до останнього моменту сподіватися, що подія не є обманом.

Важливо відзначити, що потерпілого характеризує сам злочин, жертвою якого він став. Залежно від того, в якій сфері діяв шахрай, його жертвам можуть бути притаманні такі характеристики як: схильність до азартних ігор (шахрайства з фальшивими онлайн-казино), необачність, самовпевненість, бажання легкої наживи (шахрайства з інвестиційними схемами і платіжними системами) та ін.

У тих випадках, коли злочинець для оплати товарів в інтернет-магазинах надає номера неналежних йому кредитних карт, то, відповідно до чинної світової практики роботи з кредитними картами в мережі Інтернет, ризики, пов'язані з шахрайством, несуть магазини, а не справжні власники кредитних карт. У зв'язку з цим, шкода заподіюється саме магазинам, оскільки власникам карт, в разі виявлення факту шахрайства, будуть відшкодовані їх грошові кошти.

Звісно ж, що магазини електронної торгівлі можна вважати потерпілими від шахрайства і в тих випадках, коли зловмисники використовували точну копію сайту реально існуючого магазину з метою отримання конфіденційної фінансової інформації про клієнтів магазину (наприклад, дані кредитних карт). В цьому випадку репутація магазину може постраждати. Наприклад, добре підготовлені в технічному плані шахраї, досконально вивчили механізми електронних угод, можуть зламати локальну мережу інтернет-магазину і скопіювати звідти все програмне забезпечення, включаючи бухгалтерські програми і списки імен і паролів. Після цього, увійшовши в Мережу, вони стають клонами цього магазину і можуть відслідковувати всі операції. Як тільки будь-якої нічого не підозрюючи покупець здійснить покупку, до шахраїв потрапляє інформація про його кредитну картку. Після цього злочинець, використовуючи викрадене програмне забезпечення, списує з рахунку покупця гроші за покупку ще раз і переводить їх на рахунок магазину. Після цього, знову від імені магазину, оформляє повернення. Однак гроші повертати не законному власнику, а на рахунок шахрая [65, с. 86].

Відомі випадки, коли інтернет-магазини ставали жертвами шахраїв, почасти внаслідок своєї віктимної поведінки. Тому при розслідуванні інтернет-шахрайств за участю магазинів електронної торгівлі в ролі потерпілої сторони необхідно перевірити всю доступну інформацію про угоди, проведені за час до виявлення злочину. У деяких випадках процес встановлення кола потерпілих може бути ускладнений, якщо в ролі потерпілого виступає юридична особа, оскільки такий стан, як зазначалося раніше, може завдати шкоди її діловій репутації. Звісно ж, що в даний час такі ситуації зустрічаються рідше, ніж в

минулі роки. Оскільки будь-яка організація зацікавлена в тому, щоб в майбутньому знову не стати жертвою шахраїв, то вона більш охоче буде надавати наявну інформацію правоохоронним органам. Особливо такий підхід є актуальним для банків та інших фінансових організацій, які, як правило, мають у своєму розпорядженні служби безпеки та іншими ресурси, що дозволяють відслідковувати діяльність шахраїв.

Висновок до розділу 1.

Підводячи підсумок загальній характеристиці економічних злочинів, що вчиняються в кіберпросторі, нами було зроблено наступні висновки:

1. Основні особливості здійснення шахрайства в мережі Інтернет залежать від обраної зловмисником схеми, виду шахрайства, а також сфери життєдіяльності, в якій збирається діяти злочинець. Цей вибір обумовлює спосіб реалізації злочинних намірів, а також те, в якому вигляді буде отримана кінцева вигода: грошові кошти, товари, послуги або інформація.

Всі види шахрайства в мережі Інтернет можна умовно об'єднати в такі групи: 1) засновані переважно на використанні електронної пошти та / або інших засобів обміну повідомленнями як основних інструментів впливу на жертву; 2) шахрайства, в схемах яких центральне місце відводиться застосуванню сайтів.

На жаль, своєчасне виявлення використовуваних інтернет-шахраями шкідливих програм неможливо за допомогою спеціальних засобів, оскільки компанії-виробники антивірусних та інших захисних програм не завжди встигають вчасно реєструвати нові шкідливі програми. В національній правовій науці проблеми взаємодії реальної і віртуальних економік досі в достатній мірі не вивчені. Тому дослідження такого роду шахрайства поки що можливо лише на теоретичному рівні.

Щодо характеристики особистості інтернет-шахрая, можемо вказати , що для інтернет-злочинності характерною рисою є переважання злочинців чоловічої статі. Незважаючи на те, що серед користувачів Інтернету

співвідношення жінок і чоловіків приблизно однаково, останні виявляють більш високу кримінальну активність. Однією з характерних особливостей інтернет-злочинності взагалі і інтернет-шахрайства, зокрема, є відсутність судимості (або вчинення злочину вперше) у злочинців - близько 90% всіх випадків. При розслідуванні шахрайства в мережі Інтернет рекомендується використовувати всі законні засоби для того, щоб злочинці самі приходили до висновку про необхідність співпраці зі слідством, так як в цьому випадку можна отримати максимальну кількість інформації і, відповідно, забезпечити найбільш повне і об'єктивне розслідування вчиненого діяння .

Особливостями особистості потерпілого від кіберзлочинності є наступні: З огляду на те, що інтернет-шахрайство носить корисливий характер, можна виділити наступні підгрупи потерпілих: фізичні особи, в тому числі іноземні; підприємства зв'язку і провайдери мережі Інтернет; банки; магазини електронної торгівлі; інші комерційні і некомерційні організації; інші іноземні юридичні особи; Фізичні особи формують найбільшу групу потерпілих, яка за різними оцінками складає близько 20-25% всіх злочинів в мережі Інтернет, а у випадках з шахрайством ця група, разом з іноземними фізичними особами, становить основну масу потерпілих (понад 80% від загального числа); У більшості випадків потерпілі від інтернет-шахрайства поводяться віктимно, внаслідок чого злочин стає можливим; Передумовами віктимної поведінки є такі: 1) відсутність необхідних знань і умінь користування комп'ютером, їх мережею, програмним забезпеченням; 2) недбале ставлення до конфіденційної інформації або легковажний розрахунок на те, що нічого не станеться; 3) неправильні уявлення користувача про ступінь захищеності інформації.

В незалежності від того, про який вид шахрайства в Інтернеті йде мова, характеристика кола потерпілих осіб, багато в чому, схожа. У деяких випадках процес встановлення кола потерпілих може бути ускладнений, якщо в ролі потерпілого виступає юридична особа, оскільки такий стан, може завдати шкоди його діловій репутації.

РОЗДІЛ 2. ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ЕКОНОМІЧНИХ ЗЛОЧИНІВ, ЩО ВЧИНЯЮТЬСЯ В КІБЕРПРОСТОРІ

2.1. Особливості проведення окремих оперативно-розшукових заходів

У роботах по теорії оперативно-розшукової діяльності термін оперативно-розшукові заходи (ОРЗ), на відміну від актів законодавства, використовується досить давно і широко. Після прийняття закону «Про оперативно-розшукову діяльність» 1992 року на сторінках наукової літератури з'явилося поняття оперативно-розшукового заходу, сформульоване в перших коментарях до цього законодавчого акту. Під ОРЗ пропонувалося розуміти складовий структурний елемент оперативно-розшукової діяльності, що представляє собою систему взаємопов'язаних дій, головним напрямком яких є вирішення конкретних тактичних завдань.

У теорії ОРД йде активний процес конструювання цього системоутворюючого поняття. Тим не менше, більшість наявних визначень не здатні в повній мірі відобразити основні, сутнісні ознаки оперативно-розшукових заходів. Причинами цього, на наш погляд, є відсутність наступності і, часом, недостатнє використання логічних методів у вирішенні цієї проблеми.

Інтернет як глобальну комп'ютерну мережу можна розглядати з двох підходів:

1) технологічний підхід (Інтернет як інформаційно-телекомунікаційне середовище, що забезпечує обробку та зберігання інформації);

2) соціальний підхід (Інтернет як соціально-культурне середовище, впливає на багато сторін життя суспільства і утворює специфічне середовище реалізації деяких видів діяльності і прояви суспільних відносин).

В якості нового виду соціального простору Інтернет накладає відбиток на стратегію і тактику форм ОРД, що застосовуються в розслідуваннях злочинів, скоєних в мережі Інтернет, а також створює особливі умови для здійснення ОРЗ.

У літературі вказується, що оперуючи поняттям «інформаційний простір Мережі» (іноді можна зустріти термін «Кіберпростір») можна розглядати

мережу Інтернет не тільки як систему телекомунікацій, а й як місце здійснення ОРД [64, с. 110].

Звісно ж що таке ставлення до мережі Інтернет не у всіх випадках доречно.

Важливою умовою ефективного проведення ОРЗ в Інтернеті є знання і розуміння особливостей здійснюваних в ньому злочинів. На наш погляд, для цілей цього дослідження найбільш ємним і слушним є визначення оперативно-розшукового заходу, дане А. Кузьменко, який, зокрема, розглядав його як «Складову частину оперативно-розшукової діяльності, відомості про організацію і тактику якої становлять державну таємницю, що представляє собою сукупність дій спеціально уповноважених на те державних органів та їх посадових осіб, що здійснюються з дотриманням регламентованих законом підстав та умов, що відповідає нормам моралі і моральності і безпосередньо спрямовану на досягнення цілей і дозвіл завдань оперативно-розшукову діяльність » [62, с. 54].

Необхідно відзначити, що проведення оперативно-розшукових заходів вимагає виконання певних визначених законом умов:

1. Громадянство, національність, стать, місце проживання, майновий, посадовий та соціальний стан, належність до громадських об'єднаннь, ставлення до релігії і політичні переконання окремих осіб можуть бути перешкодою для проведення щодо них оперативно розшукових заходів на території України лише тоді, коли це передбачено законом.

2. Проведення оперативно-розшукових заходів, які обмежують конституційні права людини і громадянина на таємницю листування, телефонних переговорів, поштових, телеграфних та інших повідомлень, переданих по мережах електричного і поштового зв'язку, а також право на недоторканність житла, допускається тільки на підставі судового рішення і при наявності інформації: 1) про ознаки підготовлюваного, що здійснюється або досконалого протиправного діяння, за яким ведення попереднього слідства обов'язково; 2) про осіб, що підготовляють, які роблять чи вчинили протиправне діяння, за яким ведення попереднього слідства обов'язково; 3) про

події або дії (бездіяльності), що створюють загрозу державній, військовій, економічній або екологічній безпеці України.

3. На підставі мотивованої постанови одного з керівників органу, який здійснює оперативно-розшукову діяльність, допускається проведення оперативно-розшукових заходів, які обмежують конституційні права людини і громадянина на таємницю листування, телефонних переговорів, поштових, телеграфних та інших повідомлень, переданих по мережах електричного і поштового зв'язку, а також право на недоторканність житла, з обов'язковим повідомленням суду (судді) протягом 24 годин. Протягом 48 годин з моменту початку проведення оперативно-розшукового заходу орган, його здійснює, зобов'язаний отримати судове рішення про проведення такого оперативно-розшукового заходу або припинити його проведення. При цьому необхідна наявність наступних умов: 1) мова йде про випадки, які не терплять зволікання і можуть призвести до скоєння тяжкого або особливо тяжкого злочину; 2) є дані про події та дії (бездіяльності), що створюють загрозу державній, військовій, економічній або екологічній безпеці України.

4. Прослуховування телефонних та інших переговорів допускається лише у тих осіб, які підозрюються або обвинувачуються у скоєнні злочинів середньої тяжкості, тяжких або особливо тяжких злочинів, а також осіб, які можуть мати дані про зазначені злочини. Фонограми, отримані в результаті прослуховування телефонних та інших переговорів, зберігаються в опечатаному вигляді в умовах, що виключають можливість їх прослуховування і тиражування сторонніми особами.

5. У разі порушення кримінального провадження щодо особи, телефонні й інші переговори якого прослуховуються відповідно до закону про ОРД, фонограма і паперовий носій записи переговорів передаються слідчому для залучення до кримінальної справи в якості речових доказів. Подальший порядок їх використання визначається КПК України [61].

6. У разі виникнення загрози життю, здоров'ю, власності окремих осіб за їх заявою або за їх згодою в письмовій формі дозволяється прослуховування переговорів, що ведуться з їх телефонів, на підставі постанови, затвердженої

керівником органу, що здійснює оперативно-розшукову діяльність, з обов'язковим повідомленням відповідного суду (судді) протягом 48 годин.

7. Контрольна закупка або контрольована поставка предметів, речовин і продукції, вільна реалізація яких заборонена або обіг яких обмежений, а також оперативний експеримент або оперативне впровадження посадових осіб органів, здійснюють оперативно-розшукову діяльність, а так само осіб, що надають їм сприяння, проводяться на підставі постанови, затвердженого керівником органу, що здійснює оперативно-розшукову діяльність.

8. Проведення оперативного експерименту допускається тільки з метою виявлення, попередження, припинення і розкриття злочину середньої тяжкості, тяжкого або особливо тяжкого злочину, а також з метою виявлення і встановлення осіб, їх підготовляють, які роблять чи які вчинили.

Інформація, що має визначальне значення для розкриття і розслідування шахрайства в мережі Інтернет, має три основних джерела:

по-перше, повідомлення обізнаних осіб про обставини підготовки і вчинення злочинів;

по-друге, електронні посилання на матеріали, заборонені до розповсюдження (наприклад, різні бази даних, що містять особисту, фінансову та ін.);

по-третє, сліди протиправної діяльності (наприклад, сайти-двійники, лог-файли серверів і т.д.). Також необхідну інформацію можна знайти шляхом дослідження листування по електронній пошті підозрюваних в шахрайстві осіб, журналів сервісів обміну повідомленнями в режимі реального часу (ICQ, IP-телефонія) [65, с. 87].

Необхідно зазначити, що при розслідуванні шахрайства в мережі Інтернет оперативно-розшукові заходи можуть проводитися в самому Інтернеті. Специфіку таких заходів обумовлюють три чинники: особливості кіберпростору, особливості Інтернету як особливого простору і особливості шахрайства в Інтернеті як злочину.

Розглянемо деякі оперативно-розшукові заходи з точки зору розслідування комп'ютерних злочинів взагалі і шахрайства в мережі Інтернет, зокрема.

Зняття інформації з технічних каналів зв'язку. Видається, що даний оперативно-розшуковий захід є одним з основних, що проводяться при розслідуванні не тільки шахрайства в Інтернеті, а й інших комп'ютерних злочинів. Зняття інформації з технічних каналів зв'язку вважається одним з перспективних з точки зору розвитку оперативно-розшукових заходів. В даний час технічні засоби зв'язку, наприклад Інтернет, набувають все більш поширеного характеру. При цьому активно розвиваються і інші види технічного зв'язку. Тому в літературі висловлюються припущення про те, що в майбутньому можливе розділення на законодавчому рівні зняття інформації з технічних каналів зв'язку на кілька - в залежності від виду зв'язку [68, с. 112].

Однак, на наш погляд, такий поділ буде зайвим, у всякому разі, якщо мова йде про доповнення класифікації. Звісно ж, що найбільш раціональним буде виділення різних видів розглянутого оперативно-розшукового заходу через опис особливостей їх проведення у законі про ОРД.

У конкретний момент часу інформація може знаходитися в одній з двох форм: статичній формі (зберігання на машинному носії) і динамічній формі (передача по каналу зв'язку). Зняття інформації з технічних каналів зв'язку здійснюється щодо інформації, що знаходиться в процесі передачі, через її збір в масштабі реального часу шляхом перехоплення за рахунок використання спеціального обладнання та програмного забезпечення [76, с. 43].

З урахуванням особливостей даного ОРЗ інформація, що підлягає зніманню, знаходиться в електронно-цифровій формі. Отримана інформація записується або копіюється на різні фізичні носії інформації (лазерні, жорсткі диски і ін.)

Як правило, зняття інформації з технічних каналів зв'язку, здійснюється трьома основними способами: 1) впровадженняv програмних, апаратних, апаратно-програмних пристроїв для перехоплення інформації в технічні засоби зберігання, обробки і передачі інформації з технічних каналів зв'язку; 2) перехопленням інформації на лініях зв'язку і в мережах передачі даних, а також подальше дешифрування цієї інформації; 3) впровадження програмних засобів, які порушують нормальне функціонування систем захисту інформації (в тому

числі парольно-ключових систем), що компрометують ключі і засоби криптографічного захисту інформації в цілях отримання доступу до інформації, що захищається [78, с. 14].

Зняття інформації з технічних каналів зв'язку може здійснюватися в пасивній і активній формі. Розглянемо ці форми детальніше.

Пасивне перехоплення передбачає стеження за переданими повідомленнями без втручання в їх потік. Це досягається шляхом копіювання повідомлень, які продовжують свій рух по каналах інтернет-зв'язку до пункту призначення. Головною перевагою пасивного перехоплення є високий рівень конспірації, оскільки викликана копіюванням затримка при передачі повідомлення вкрай мала і, таким чином, відправник і одержувач не помічають ознак перехоплення.

Активне перехоплення має на увазі здійснення певних дій з інформацією, що передається, наприклад зміна змісту, затримання і т.д. Також, з огляду норми закону про ОРД, можна говорити про повне блокування передачі повідомлень щодо конкретних осіб з метою недопущення отримання ними певної інформації. Оскільки активне перехоплення пов'язане з впливом на передану інформацію, є сенс говорити про низький ступінь конспірації і, як наслідок, зняття інформації з технічних каналів зв'язку в даній формі не завжди виправдано, оскільки шахраї часто діють обережно і при перших ознаках серйозної небезпеки можуть припинити свою діяльність [68, с. 112] .

Звісно ж, що в такому випадку подальше розслідування буде істотно ускладнено, оскільки може бути загублена частина слідів, що вказують на злочинців і їх діяльність (наприклад, закриття грошових рахунків, видалення сайтів, спроби зникнення шахраїв з поля зору правоохоронних органів і т.д.).

Інформація, отримана в процесі зняття інформації з технічних каналів зв'язку, за своїм змістом поділяється на дві складові частини: службова (інформація про маршрут передачі) і змістовна. Як правило, для вирішення оперативно-розшукових завдань в ході розслідування інтернет-шахрайства, головну цінність має змістовна частина повідомлень як потенційне джерело відомостей про злочинну діяльність. Вважаємо за необхідне відзначити, що в

деяких випадках службова частина перехоплюваних повідомлень також відіграє серйозну роль, оскільки її аналіз може допомогти визначити місце знаходження шахрая (або одного з групи злочинців).

Зняття інформації з технічних каналів зв'язку можливо не тільки по каналах передачі даних, але також по електромагнітнимх і інших полях, випромінюваних пристроями, сполученими з комп'ютером (роутери, пристрої, що використовують технологію Bluetooth для зв'язку з комп'ютером і т.д.). Однак в цьому випадку потрібне технічне забезпечення суб'єктів розслідування спеціальними інструментами. Як приклад вважаємо доречним привести розроблене швейцарською компанією Dreamlab Technologies пристрій під назвою Keykeriki 2, що має функцію перехоплення даних з бездротових пристроїв і систем (наприклад, бездротових клавіатур) [81, с. 758].

Звісно ж, що застосування таких технічних засобів доречно, в основному, в тих випадках, коли шахрай, або один із співучасників шахрайства використовує комп'ютери всередині компанії, яка постраждала від шахрайства (або здатної постраждати, якщо мова йде про діяльність щодо запобігання підготовлюваного злочину).

Застосування подібних пристроїв для перехоплення інформації в житлі передбачуваного шахрая, на наш погляд, має сенс в тих випадках, коли розслідується велике шахрайство, в результаті якого може бути завдано великої шкоди невизначено широкому колу осіб (як юридичних, так і фізичних).

Оскільки досліджуваний оперативно-розшуковий захід обмежує конституційне право на таємницю зв'язку і кореспонденції [53], його застосування можливе на підставі судового рішення або мотивованої постанови відповідного керівника органу, що здійснює ОРД, з обов'язковим отриманням судового рішення про проведення даного заходу протягом 48 годин.

При цьому виникають певні проблеми. Справа в тому, що при знятті інформації з технічних каналів зв'язку представляє деяку складність виділення із загального потоку отриманих даних тих повідомлень, які відносяться до передбачуваних шахраїв. Дана проблема особливо актуальна, якщо мова йде про багато користувачів, оскільки одне і те же ідентифікаційне ім'я може бути

доступно різним користувачам (так само як і один користувач може ховатися за кількома іменами).

Таким чином, виходячи зі сказаного вище, вважається можливим дати наступне визначення досліджуваного оперативно-розшукового заходу. Зняття інформації з технічних каналів зв'язку (з точки зору розслідування шахрайства в мережі Інтернет) - це регламентований законом про ОРД оперативно-розшуковий захід, що проводиться на підставі судового рішення, що полягає в негласному зніманні інформації, переданої по мережах електричного зв'язку, комп'ютерним та іншим мережам, шляхом контролю спеціальними технічними засобами і програмним забезпеченням роботи відповідних пристроїв і систем, а також випромінюваних ними електромагнітних та інших полів.

Незважаючи на те, що правоохоронні органи, як зазначалося вище, можуть залучати до співпраці компанії, що надають послуги зв'язку, ми наполягаємо на доцільності лише негласного характеру зняття інформації як оперативно-розшукового заходу. На це є кілька причин. По-перше, не завжди компанії-провайдери ставляться до відома про проведений оперативно-розшуковий захід. По-друге, навіть якщо ці компанії залучені до співпраці в розслідуванні шахрайства, вони не мають у своєму розпорядженні всією інформацією про те, які саме дії будуть здійснювати суб'єкти розслідування в ході проведення заходу. По-третє, в Законі про ОРД чітко вказується всім особам, залученим до підготовки або проведенню оперативно-розшукових заходів, тримати в таємниці відомості, які стали їм відомі у ході підготовки або проведення оперативно-розшукових заходів. До заходу можуть також залучатися співробітники організацій -власників технічних каналів зв'язку і відповідної інформації (наприклад, компанії-провайдери, що надають доступ в Інтернет).

До числа особливостей даного заходу відноситься те, що інформація, яка підлягає зніманню знаходиться в електронно-цифровій формі. Отримані відомості записуються на різні носії інформації .

Зняття інформації з технічних каналів інтернет-зв'язку проводиться оперативними співробітниками оперативно-розшукових органів, з використанням оперативно-технічних сил і засобів органів служби безпеки,

органів внутрішніх справ та органів з контролю за обігом наркотичних засобів і психотропних речовин. Як було сказано вище, до заходу можуть також залучатися співробітники організацій - власників технічних каналів і відповідної інформації.

Результати зняття інформації відображаються в рапорті або довідці, яка складається оперативним співробітником, до яких додаються відповідні носії (поміщені в упаковку і опечатані) з отриманою інформацією, а також, якщо це необхідно, роздруківки цієї інформації.

На сьогоднішній день великою популярністю користується так до звана IP-телефонія. Причому нерідко трапляється, коли такий вид зв'язку комбінується зі звичайним і/або мобільним телефонним зв'язком. В цьому випадку необхідно говорити не тільки про зняття інформації з технічних каналів зв'язку, а й про такий оперативно-розшуковий захід, як прослуховування телефонних розмов. Отже, в таких ситуаціях необхідно враховувати вимоги, що пред'являються не тільки до зняття інформації з технічних каналів зв'язку, а й до прослуховування телефонних переговорів.

Прослуховування телефонних переговорів з підключенням до станційної апаратури підприємств, установ і організацій проводиться з використанням оперативно-технічних сил і засобів органів служби безпеки, органів внутрішніх справ та органів з контролю за обігом наркотичних засобів і психотропних речовин. Прослуховування телефонних переговорів, як і інші оперативно-розшукові заходи, що обмежують конституційні права людини і громадянина на таємницю листування, телефонних переговорів, поштових, телеграфних та інших повідомлень, переданих по мережах електричного і поштового зв'язку, а також право на недоторканність житла, допускається на підставі судового рішення і то при наявності визначеної інформації, описувати яку через обмеженість обсягу нашого дослідження не будемо.

Здійснення прослуховування телефонних переговорів на дротяних лініях зв'язку можливо на різних ділянках каналу зв'язку - як на станційній апаратурв операторів зв'язку, так і на самій лінії. Прослуховування телефонних переговорів на бездротових лініях зв'язку (стільниковий зв'язок, радіозв'язок,

зв'язок через супутники, що обертаються на низьких орбітах; зв'язок інтегрального обслуговування (наприклад, відеоконференції) може здійснюватися шляхом підключення до станційної апаратури операторів зв'язку і шляхом сканування сигналу, що йде до засобу зв'язку, тобто до телефону.

Прослуховуватися може зв'язок як одностороній (спілкування по черзі), двосторонній, так і багатосторонній (конференцзв'язок); як засіб зв'язку, що належить певній особі (стаціонарний, стільниковий телефон), так і засіб зв'язку, встановлений в певному місці, де буває підозрювана особа. Прослуховуванню підлягає розмова всіх абонентів, оскільки прослуховування тільки одного з них (наприклад, шляхом зняття вібрацій віконного скла, що коливається від розмови абонента) буде не прослуховуванням, а наглядом з використанням спеціальних технічних засобів.

У тих випадках, коли для розслідування інтернет-шахрайства необхідна додаткова допомога, правоохоронні органи мають право залучити для проведення оперативно-розшукового заходу осіб, безпосередньо не пов'язаних з правоохоронною діяльністю, наприклад операторів зв'язку. Порядок взаємодії органів, які здійснюють оперативно-розшукових діяльність, з уповноваженим органами виконавчої влади в галузі зв'язку в питанні прослуховування телефонних переговорів здійснюється на підставі двосторонніх угод між ними [76, с. 43].

Результати прослуховування також відображаються рапорті або довідці, які складаються оперативним співробітником, до яких додаються отримані фонограми, які зберігаються в опечатаному вигляді в умовах, що виключають можливість їх прослуховування і тиражування сторонніми особами. Надалі фонограми можуть бути направлені на експертизу для визначення їх автентичності (відсутність монтажу), складання протоколу про прослуховування і можливість використовуватись як доказ.

При розслідуванні деяких інтернет-шахрайств може виникнути необхідність отримання доступу до певної інформації, що зберігається в комп'ютері шахрая, підключеного до мережі Інтернет (наприклад, інформація про вчинені або підготовлювані злочини, локальні лог-файли програм

миттєвого обміну повідомленнями з листуванням передбачуваного злочинця і т.д .). На перший погляд, подібне дослідження можна віднести до зняття інформації з технічних каналів зв'язку, однак, в силу наступних обставин, таке твердження буде не вірним:

1. Зняття інформації з технічних каналів зв'язку здійснюється щодо інформації, що знаходиться в динамічному стані в каналах зв'язку. В даному ж випадку мова йде про інформацію, що зберігається в комп'ютері шахрая, яку він, можливо, не буде передавати будь-кому.

2. Доступ до комп'ютерної системи шахрая здійснюється дистанційно. У випадку ж із зняттям інформації з каналів зв'язку існує можливість більш близького контакту з досліджуваним об'єктом (наприклад, для установки спеціального обладнання або програмного забезпечення).

Подібну дію уявляється можливим ототожнювати з обстеженням приміщень, будівель, споруд, ділянок місцевості і транспортних засобів, оскільки, не дивлячись на те, що мова йде про локально збережені дані, доступ до них буде здійснюватися дистанційно, тобто буде відбуватися проникнення в систему з подальшим вивченням наявних в ній даних.

Обстеження приміщень, будівель, споруд, ділянок місцевості і транспортних засобів як оперативно-розшуковий захід пов'язане з вивченням обстановки для виявлення слідів злочинної діяльності інтернет-шахраїв і виявлення предметів і документів (в тому числі електронних), що мають відношення до розслідуваного злочину, а також їх фіксація і збереження для вирішення завдань розслідування.

Досліджуваний оперативно-розшуковий захід задає специфіку розшукуваної інформації. Справа в тому, що мова йде про інформацію, що міститься в специфічних матеріальних носіях, які, будучи продуктом високих технологій (жорсткі диски, карти пам'яті, лазерні диски і т.д.), далеко не завжди пристосовані для перебування в незахищеному або погано захищеному середовищі. Тому, на наш погляд, доцільно обмежити коло обстежуваних об'єктів. Можна опустити відкриті ділянки місцевості, оскільки під впливом природних явищ ймовірність псування носіїв інформації (навіть якщо створили

схованку) велика. До того ж мова може йти і про обладнання, що використовується шахраями, придбати яке досить проблематично (сканери і пристрої для створення підроблених кредитних карт, наприклад).

Доцільно також виключити споруди, оскільки шахрайство в мережі Інтернет, на відміну від традиційного шахрайства, часто не вимагає активних пересувань з боку злочинця. Те ж частково відноситься і до транспортних засобів, хоча тут вважаємо за необхідне зазначити, що в деяких випадках обстеження транспортного засобу, яким користувався шахрай, може принести користь [68, с. 112].

Наприклад, якщо в ході розслідування інтернет-шахрайства встановлено, що доступ до одного з постраждалих об'єктів (наприклад, інтернет-магазин) здійснювався в межах одного населеного пункту, але з великої кількості місць, то можна припустити, що шахрай, перед вчиненням злочину, їздив по населеному пункту, скануючи місцевість з метою виявити точки бездротового доступу. Отже, є ймовірність, що в транспортному засобі знаходиться відповідне обладнання: портативний комп'ютер, ОРБ-приймач, антени прийому і т.д. В цьому випадку ОРБ -приймач може містити інформацію про маршрут пересування, а комп'ютер - інформацію про знайдені точки доступу та їхні розташування. Слід, однак, проявляти обережність при дослідженні комп'ютера, що належить шахраю, оскільки, якщо він має високий рівень знань і підготовки в роботі з комп'ютером і мережею Інтернет, він може передбачити механізм відстежування будь-яких (навіть невдалих) спроб проникнення в систему і будь-яка підозріла інформація може сполохати шахрая, навіть якщо він не знайде підтверджень своїм побоюванням. Тому, якщо в ході проведення даного оперативно-розшукового заходу необхідно встановити спеціальні програми (наприклад, програмний перехоплювач сигналів з клавіатури), потрібно зробити це, залишивши якомога менше слідів.

Для досягнення цієї мети рекомендовано якомога тісніше співпрацювати з фахівцями в сфері інформаційних технологій. В даний час існує велика кількість доступних кожному користувачеві ПК засобів для індивідуалізації використовуваного програмного забезпечення, аж до створення власної версії

операційної. Тому консультація фахівця (наприклад, по операційним системам) є грамотним і необхідним рішенням слідчого, тому що отримана інформація дозволить максимально якісно виконати оперативно-розшуковий захід, залишивши мінімальні сліди присутності в системі підозрюваного в інтернет-шахрайстві.

Збір зразків для порівняльного дослідження є оперативно-розшуковим заходом, що полягає у вилученні, отриманні предметів з метою їх подальшого оперативно-розшукової розпізнавання або ідентифікації. Даний захід має схожість з отриманням зразків для порівняльного дослідження (ст. 245 КПК України [61]), проте до нього (збору зразків для порівняльного дослідження) не застосовуються процесуальні вимоги, і воно може здійснюватися негласно. До зібраних зразків прийнято відносити традиційні криміналістичні об'єкти: відбитки пальців рук, волосся, взуття та її сліди, одяг, запахові сліди тощо Можуть збиратися зразки почерку, підпису (в тому числі і цифрового), набраного на комп'ютері тексту (для авторознавчої експертизи), зразки продукції, напівфабрикатів і т.д. (Наприклад, заготовки кредитних карт або носіїв інформації з дампами пам'яті цих карт, підроблені цінні папери та ін.).

До проведення заходу можуть залучатися експерти і особи, що володіють відповідними спеціальними знаннями, а також застосовуватися технічні засоби.

Чимала частина вчених-криміналістів пов'язують збір зразків для порівняльного дослідження з матеріальними предметами [81, с. 759]. Однак з розвитком злочинності в сфері високих технологій стало актуальним збір зразків комп'ютерних програм. Комп'ютерні програми, в тому числі, різні шкідливі програми, не є матеріальними предметами. Проте, закон про ОРД перелік зібраних зразків залишає відкритим. Збір комп'ютерних програм для їх дослідження в даний час досить поширений.

Крім комп'ютерних програм, до числа допустимих зразків вважаємо обґрунтованим віднести інші файли, наприклад аудіо-файли, бази даних і ін. файли. Подібні об'єкти можуть бути знаряддями злочинів (генератори номерів кредитних карт, шкідливі програми і т.д.), містити інформацію, відкрите поширення якої заборонено (бази даних платників податків, кредитні історії і

т.д.), зберігати сліди злочинів (наприклад, журнали реєстрації подій в комп'ютерній системі або на сервері) або вказувати на об'єкти, що мають доказове значення (файли журналів листування).

Спостереження - це негласне стеження за особами, що цікавлять слідство, в тому числі причетними до вчинення кримінальної події, використовувані ними транспортні засоби, з метою отримання значимої інформації (наприклад, про організацію злочинної групи інтернет-шахраїв, взаємини її членів, способи фінансування групи і т.д.).

Розрізняють три види спостереження: 1) фізичне; 2) електронне; 3) комплексне.

До фізичного спостереження, основа якого - візуальний спосіб стеження, відноситься діяльність співробітників, що спеціалізуються на цих методах роботи, що здійснюється або самим співробітником, або іншими особами за його завданням. В ході фізичного спостереження можливе застосування різних технічних засобів - фотоапаратів, відеокамер, які дозволяють фіксувати дії спостережуваного особи в реальному масштабі часу.

Засноване на застосуванні спеціальних технічних засобів електронне спостереження, дозволяє організовувати і проводити спостереження за особою як в приміщенні, так і в транспортному засобі, на відкритій місцевості тощо. При цьому залучаються, як правило, співробітники оперативно-технічних підрозділів. В ході цього виду спостереження часто використовується апаратура аудіо-, відеозапису для контролю і запису розмов, дій і операцій особи, що перевіряється [85].

Комплексне спостереження дозволяє фіксувати в хронологічному порядку, в реальному часі, всю життєдіяльність особи, що перевіряється протягом усього часового інтервалу, протягом якого здійснюється цей захід. При цьому рекомендується залучати до сприяння відповідних фахівців, що дозволить більш якісно провести оперативно-розшуковий захід. Наприклад, фахівець здатний використовувати спеціальні технічні засоби з набагато більшою результативністю, ніж це б зробили слідчий або інша особа.

2.2. Тактичні особливості допиту обвинуваченого та потерпілого від економічних злочинів, що вчиняються в кіберпросторі

Згідно ст. 42 КПК України, Оообвинуваченим (підсудним) є особа, обвинувальний акт щодо якої переданий до суду [61] .

Звісно ж, що тактика допиту обвинуваченого - одна з найбільш складних. Вона повинна відповідати вимогам кримінально-процесуального закону, будуватися в залежності від складу злочину, особи обвинуваченого, наявних у справі доказів, від того, визнає обвинувачений себе винним у пред'явленому йому обвинуваченні чи ні.

Розуміння і прогнозування поведінки підозрюваного (обвинуваченого) в інтернет-шахрайстві мають особливу значимість в тактиці допиту, який є процесуальною формою міжособистісного спілкування.

Ми вважаємо правильною думку деяких дослідників, які, зокрема, вказують, що адаптація попереднього розслідування до умов реального пріоритету особистості являє актуальну проблему криміналістики [100, с. 184]. Основним напрямком вирішення даної проблеми бачиться «психологізація» криміналістичної тактики, тобто озброєння слідчого ефективними прийомами проведення слідчих дій. Особливо такі прийоми повинні бути затребувані при допиті підозрюваних і обвинувачених у справах про шахрайство в мережі Інтернет, який обґрунтовано вважається найбільш психологічно складною слідчою дією. Поєднання даних особливостей обумовлено тим, що принципово значуща інформація про підготовку, вчинення і приховування шахрайства знаходиться в психіці підозрюваного (обвинуваченого), який часто є єдиним володільцем цих відомостей і часто активно протидіє їх виявленню і процесуальному оформленню.

Оскільки переважна більшість інтернет-шахраїв - особи, що вперше вчинили злочин, то розумним при їх допиті представляється застосування рекомендацій щодо ведення допитів осіб, які вперше скоїли шахрайство, проте з урахуванням їх інтелектуального розвитку та специфічних знань в сфері сучасних інформаційних технологій.

При проведенні допиту підозрюваного / обвинуваченого за доцільне дотримуватися наступних рекомендацій.

На початку допиту, на стадії вільної розповіді, слідчому рекомендується найбільш докладно фіксувати інформацію, отриману від допитуваного інтернет-шахрая, оскільки її можна буде використовувати в питально-відповідній стадії (наприклад, для викриття у брехні, якщо у слідчого будуть відповідні підозри).

Після закінчення стадії вільної розповіді слідчий ставить запитання допитуваному (питально-відповідна стадія). Звісно ж необхідним в даному випадку вказати, що на наш погляд, на конкретні формулювання питань, а також їх кількість, вирішальний вплив надає конкретний підвид інтернет-шахрайства (фінансова піраміда, фіктивні сайти знайомств і т.д.).

Психічний стан, мотиви дій, особистісні якості допитуваних визначають їх поведінку на досудовому слідстві і, тим самим, зумовлюють психологічний підхід до них, обрання найбільш ефективних тактичних і психологічних прийомів. В ході проведення допиту обвинувачений в інтернет-шахрайстві може відчувати найрізноманітніші почуття.

Суб'єкт, що вчинив злочинне діяння відчуває страх перед викриттям і подальшим покаранням, що, як правило, пригнічує психіку, пригнічує волю допитуваного обвинуваченого, перешкоджає адекватній оцінці обставин, що склалися, погіршує самоконтроль, а також призводить до депресивного стану. Звісно ж, що страх зазвичай виникає в осіб, які вчинили злочин, набагато раніше притягнення їх до кримінальної відповідальності. Такі психологічні стани ускладнюють встановлення психологічного контакту при допиті, а також знижують ефективність тактичних прийомів ведення допиту обвинуваченого в інтернет-шахрайстві [110, с. 384].

Для окремих обвинувачених в скоєнні інтернет-шахрайства типова страх втрати досягнутого ними положення (соціального, службового, матеріального). Тому на допиті такі обвинувачені найчастіше ухиляються від дачі правдивих показань. У такому випадку для подолання зазначеного психологічного стану

обвинуваченого необхідно переконати його в можливості відновити колишнє соціальне становище.

Звісно ж, що сильним психологічним станом, формує мотиви поведінки обвинувачуваного, є страх позбавлення волі, звичного способу життя, небажання опинитися серед злочинців. Таке відчуття, особливо властиве особам, вперше залученим до кримінальної відповідальності, зазвичай призводить їх в стан глибокої депресії.

У такій ситуації обвинувачений в інтернет-шахрайстві вважає, що уникнути затримання, арешту, утримання під вартою, вироку, пов'язаного з позбавленням волі, можна, лише заперечуючи свою провину. При наданні неправдивих свідчень у нього виникає відповідний психологічний стан, формується позиція, яку слідчому необхідно подолати. У такій ситуації необхідно переконати обвинувачуваного, що доведення провини мало залежить від його визнання, а вирішальною мірою - від усієї сукупності зібраних у кримінальній справі доказів. Також потрібно роз'яснити, що щире розкаяння і активне сприяння розкриттю всіх епізодів інтернет-шахрайства є для суду обставиною, яка пом'якшує відповідальність. Але при цьому варто акцентувати увагу на тому, що співпрацювати зі слідством необхідно вже на стадії досудового розслідування. Практика показує, що в злочинах, скоєних групою шахраїв, обвинувачений по-різному ставиться до співучасникам. Якщо комусь він багато чим зобов'язаний, то може робити спроби приховати причетність до скоєного цієї людини, сподіваючись на його відповідну допомогу і підтримку. Часто система психологічних відносин у злочинній групі інтернет- шахраїв побудована на підпорядкуванні, силі, страху, інших низинних спонукань і інстинктах. Тому в процесі розслідування, коли учасники злочинної групи шахраїв ізольовані один від одного, побудовані на такій основі відносини розпадаються.

Ефективність допиту багато в чому залежить від того, в якому психологічному стані перебуває допитуваний, від усвідомлення обвинувачуваним шахраєм своєї провини, від готовності дати правдиві свідчення. Слідчий повинен вміти грамотно комбінувати і застосовувати

тактичні прийоми ведення допиту, щоб послабити або нейтралізувати негативні психологічні стани і посилити, підтримати позитивні.

Оскільки шахраї володіють «живим» розумом, то якщо вони вирішили протидіяти слідству, основною зброєю слідчого повинен стати інтелект, кінцевою метою застосування якого повинно стати викриття допитуваного у брехні, постановка перед єдино можливим виходом - співпрацювати зі слідством. З цією метою вважаємо за доцільне застосовувати такі тактичні прийоми: 1) пред'явлення наявних у розпорядженні судових доказів; 2) створення у обвинуваченого уявлення про те, що слідчий більш інформований, ніж це є насправді; 3) зміна темпу допиту; 4) маскування головного питання другорядними, що дозволить викрити допитуваного шахрая у брехні, якщо відповіді будуть не пов'язані логічно; 5) роз'яснення допитуваному можливості встановлення даного факту шляхом проведення судової експертизи; 6) маскування слідчим конкретних цілей допиту; 7) створення слідчим легенди і раптове її викриття після пояснень допитуваного і ін.

Застосування даних прийомів покликане послабити опір обвинуваченого в шахрайстві в Інтернеті шляхом виявлення невідповідностей в його свідченнях.

При розслідуванні економічних злочинів, вчинених в кіберпросторі, важливе значення має і допит потерпілих. Варто відзначити, що при будь-якому допиті необхідною умовою є довіра між слідчим і допитуваним особою, встановлення якого в досить великій кількості випадків представляє труднощі.

Як було сказано вище, потерпілі від шахрайства в мережі Інтернет найчастіше схильні приховувати не тільки окремі факти, що свідчать про скоєний діяння, а й взагалі приховувати свій статус. У таких ситуаціях доцільно говорити про конфлікт потерпілого і слідчого, здатний прийняти форму суперництва [112, с. 125]. Таке відбувається з різних причин, наприклад при неадекватної оцінки потерпілим обставин скоєння злочину. Причина може полягати також в неправильній оцінці слідчим стану потерпілого і його показань.

Як зазначається в науковій літературі, основним засобом подолання несумлінності потерпілого має виступати переконання. Наприклад,

Шавиркін Б. В. вказує, що «слідчий повинен прагнути до того, щоб потерпілий вільно і свідомо обрав позицію, спрямовану на надання сприяння у встановленні істини у кримінальній справі» [112, с. 125].

При допиті потерпілого, який прагне приховати свій статус або перешкодити встановленню істини у кримінальній справі за доцільне керуватися наступними рекомендаціями.

Проведення короткої бесіди перед початком допиту на сторонні теми. Звісно ж, що дана рекомендація застосовується до багатьох видів допиту, оскільки дозволяє отримати уявлення про особистість допитуваного, наприклад, про його освіту, моральні цінності, спосіб життя і т.д. Це дозволить визначити приблизний перелік причин, за якими потерпілий не зацікавлений в успішному розслідуванні справи. Слід також зазначити, що проведення короткої бесіди перед допитом дозволяє розрядити обстановку, допомогти в створенні довірчих відносин між учасниками допиту.

З'ясування конкретних мотивів протидії слідству. У деяких випадках можлива пряма постановка питання про причини відмови від показань або навмисного їх спотворення. Якщо це пов'язано, наприклад, з недовірою до роботи правоохоронних органів, то можна запропонувати потерпілому оцінити роботу слідчого і зібраних на даний момент матеріалів. Також представляється корисним пояснення потерпілому, що його поведінка перешкоджає захисту його ж власних прав та інтересів. Якщо потерпілих багато, доцільно роз'яснити, що своїми показаннями потерпілий допоможе не тільки швидше і якісніше розслідувати злочин, але і повернути викрадене інтернет-шахраями не тільки собі, а й іншим потерпілим. В цьому випадку у допитуваного може виникнути відчуття позитивної відповідальності перед іншими потерпілими, що дозволить знизити протидію слідчому.

Помірно співчуваюче ставлення з боку слідчого передбачає таку поведінку і стиль спілкування слідчого з потерпілим, при якому у останнього створюється стійке враження про те, що до розслідування його кримінальної справи підходять серйозно. Слідчому потрібно показати, що він щиро співчуває

потерпілому. Природно, при цьому недопустима яка б то не була фамільярність і зайва емоційність.

Повторне нагадування про відповідальність за відмову від дачі показань і дачу завідомо неправдивих показань. Дана рекомендація спрямована на створення у допитуваного почуття позитивної відповідальності. Незважаючи на те, що слідчий перед початком допиту вказує на можливість настання відповідальності, проте, якщо існує ситуація, при якій взаємної довіри між слідчим і допитуваним не виникло, то можна вдатися до акцентування уваги останнього на те, що він, в будь мірі, може з потерпілого перетворитися на обвинуваченого, оскільки відмова від дачі показань та дача завідомо неправдивих показань тягне настання кримінальної відповідальності. Звісно ж, проте, що подібна інформація особливо висловлена у формі погрози, може звести нанівець всі зусилля слідчого по створенню довірчих відносин з допитуваним. Тому, на наш погляд, згадка про можливість погіршення становища потерпілого можна використовувати тільки в крайніх випадках.

Якщо стає очевидним, що потерпілий має цінну для слідства інформацію, але намагається приховати її не дивлячись ні на що, необхідно здійснити наступні тактичні прийоми, які дозволять поставити допитуваного в такий стан, коли йому не залишиться нічого іншого, як сказати правду:

1) виклад відомих слідчому подій в різній послідовності;

2) непомітне зміщення акцентів при допиті;

3) маскування головного питання серед другорядних;

4) прохання до потерпілого від інтернет-шахрайства максимально деталізувати свої показання;

5) пред'явлення наявних у слідчого доказів у кримінальній справі [71, с. 10].

Слід, однак, враховувати положення допитуваної особи. Наприклад, якщо він є службовцям банку, а кримінальну справу порушено за фактом шахрайства з кредитними картами, то цілком можливо, що відомості, які він приховує, можуть бути пов'язані з банківською таємницею. У таких випадках необхідно більш ретельно підходити до підготовки і проведення допиту. Корисним буде

детально роз'яснити, що інформація, отримана на допиті, не буде передана стороннім особам.

2.3. Тактика обшуку

Проведення обшуку можливо на будь-якій стадії досудового розслідування. При розслідуванні діяльності злочинних груп інтернет-шахраїв обшуки найчастіше проводяться відразу ж після порушення кримінального провадження, що є виправданим і необхідним, оскільки це дозволяє виявити і вилучити речі, цінності, гроші, які є предметом злочинного посягання, виявити знаряддя злочину, затримати шахрая.

Обшуки на наступних етапах можливі при розслідуванні злочинів, вчинених у сфері економіки, коли обшуку передує тривала робота - встановлення місця та осіб, щодо яких необхідно провести обшук: документи, носії комп'ютерної інформації, пластикові карти, апаратура для роботи з пластиковими картами і т.п.

При обшуку потрібно враховувати ту обставину, що його проведення найчастіше пов'язано з вторгненням в житлове чи інше приміщення, тобто ця дія обмежує деякі конституційні права громадянина [53]. Для проведення обшуку завжди повинні бути вагомі, або, як сформульовано в законі, "достатні підстави". Говорячи про достатні підстави, законодавець мав на увазі, що слідчий повинен мати інформацію, що не викликає у нього сумнівів. Така інформація може бути отримана з різних джерел як шляхом проведення слідчих дій, так і оперативних заходів відповідно до Закону про ОРД. Джерелами фактичних даних, з яких випливає необхідність проведення обшуку, можуть бути:

а) показання свідків, потерпілих, підозрюваних, самих обвинувачених у справі про інтернет-шахрайстві;

б) заяви громадян;

в) офіційні повідомлення посадових осіб державних, громадських, комерційних організацій;

г) дані, зібрані методами оперативно-розшукової діяльності [66, с. 137]. Найкращим варіантом може вважатися такий, коли є достовірна інформація, хто конкретно, що саме і де ховає.

Обшук проводиться на підставі ухвали слідчого судді місцевого загального суду, в межах територіальної юрисдикції якого знаходиться орган досудового розслідування [62]. Подібний порядок повинен розцінюватися, крім усього іншого, як одна з гарантій захисту конституційних прав і свобод громадян.

Поряд з учасниками обшуку, тобто безпосередніми виконавцями тих чи інших дій, вважаємо за необхідне окреслити коло осіб, присутніх під час обшуку.

В першу чергу це поняті, присутність яких обов'язково за законом. Якщо обшук проводиться одночасно в декількох місцях, то в кожному повинно бути по два понятих. В їх завдання входить уважне спостереження за всіма діями учасників обшуку з тим, щоб в подальшому вони могли об'єктивно засвідчити, ким і які дії проводилися, що і де було виявлено в результаті цих дій. Подібним свідченням є підписання ними протоколу обшуку, а також, в разі необхідності, показання в ході допиту на слідстві і / або в суді. Для виконання понятими даного завдання їм повинна бути надана реальна можливість безпосереднього спостереження за діями учасників обшуку.

Відповідно до порядку, встановленого законом, має бути забезпечена присутність особи, у якої проводиться обшук, або повнолітніх членів його сім'ї. Якщо це неможливо, то запрошуються представники житлового управління або місцевих органів управління (адміністрації).

У тих випадках, коли обшук проводиться в установі, необхідна присутність його представника або його заступника (за відсутності першого). Якщо в приміщенні, де проводиться обшук, виявляться сторонні, слідчий вправі заборонити їм залишати місце обшуку до його закінчення, а також спілкуватися один з одним або іншими особами. Особам, присутнім при обшуку, слідчий зобов'язаний роз'яснити їх права бути присутніми при всіх його діях і робити заяви (які заносяться до протоколу) з приводу цих дій. У протоколі вказується, що кожному були роз'яснені його права.

Найчастіше слідчий не має повного уявлення про все, що може перебувати в місці обшуку і мати відношення до справи про кіберзлочинність. Звідси його рішення - продовжувати обшук, прагнучи виявити важливі для справи предмети, документи та інші об'єкти. Не можна ігнорувати і те, що обшукуваний нерідко з готовністю і швидко видає шукане, сподіваючись таким чином запобігти подальшому пошуку і приховати що-небудь більш важливе для слідства.

При відмові видати об'єкти добровільно, відкрити замкнені приміщення і сховища слідчий має право розкривати такі приміщення. При цьому він повинен прагнути не завдавати будь-яких зайвих пошкоджень.

Виявлені речі і документи слідчий пред'являє понятим, звертаючи їхню увагу на місце виявлення, наявності схованок, що маскують об'єктів і т.п.

Кримінально-процесуальний кодекс не забороняє проведення повторного обшуку в тому ж місці і у тих же осіб, але як виняток і за наявності вагомих підстав. Такими підставами можуть стати відомості про невиявлених тайниках, що розшукувані об'єкти, які раніше були відсутні в місці обшуку, в даний час туди доставлені.

Груповий обшук - це проведення декількох обшуків в одній справі, у різних осіб, в різних місцях в один і той же час. Застосовуваний при розслідуванні діяльності злочинних структур, цей обшук створює ефект раптовості і часто призводить до позитивних результатів. Мета групового обшуку визначається завданнями, які ставить перед собою слідча група. Об'єкти пошуку значною мірою залежать від спеціалізації злочинного формування (в сфері економіки, у сфері банківської діяльності і т.д.).

На повторний і груповий обшук поширюються всі положення закону про порядок проведення обшуку.

Тактика проведення обшуку складається з чотирьох стадій: підготовчої, оглядової, детальної та стадії фіксації результатів обшуку [62]. У свою чергу кожна з цих стадій характеризується комплексом тактичних прийомів, покликаних забезпечити успіх обшуку.

Важливими в тактичному відношенні є систематичність і акуратність пошуку. Перш за все, це означає граничну уважність під час обшуку, його цілеспрямоване проведення, здатність не відволікатися. Звісно ж, що найбільш важлива інформація про скоєне шахрайство може зберігатися на окремому від комп'ютера носії, який буде захований. Тому, якщо слідчий проявить неуважність, можуть бути пропущені ті місця, де зберігаються заховані носії.

В ході проведення обшуку, особливо в детальної стадії, слідчому бажано постійно взаємодіяти з фахівцем, який здійснює допомогу у виявленні слідів злочину, пов'язаних з використанням комп'ютерів, а також консультує членів групи з питань, пов'язаних і інформаційними технологіями, що мають відношення до справи.

За результатами обшуку складається протокол [62], вилучаються необхідні предмети. У разі необхідності вилучення комп'ютера, слідчий повинен вдатися до допомоги фахівця, щоб коректно завершити роботу системи (якщо комп'ютер працював на момент проведення обшуку) і не втратити важливу інформацію. При неможливості на місці вирішити питання про вибір правильного способу завершення роботи системи, фахівець повинен повідомити про це слідчому з метою вжиття заходів щодо транспортування комп'ютера у включеному стані, якщо це можливо (наприклад, якщо обшукуваний підозрюваний в інтернет-шахрайстві використовував пристрій безперебійного живлення). Згодом створюються «клони» вилучених носіїв інформації, інформацію в яких вивчають експерти.

Висновок до розділу 2.

Аналізуючи особливості розслідування економічних злочинів, вчинених в кіберпросторі, нами було винесено наступні висновки:

З огляду на специфіку злочинності в кіберпросторі, оперативно-розшукові заходи можна класифікувати за різними ознаками. Оперативно-розшуковий захід - складова частина оперативно-розшукової діяльності, відомості про організацію і тактику якої складають державну таємницю, що представляє

собою сукупність дій спеціально уповноважених на те державних органів та їх посадових осіб, що здійснюються з дотриманням регламентованих законом підстав та умов, що відповідає нормам моралі і безпосередньо спрямовану на досягнення цілей і вирішення завдань оперативно-розшукової діяльності.

Зняття інформації з технічних каналів зв'язку (з точки зору розслідування шахрайства в мережі Інтернет) - це регламентований законом про ОРД оперативно-розшуковий захід, що полягає в негласному зніманні інформації, переданої по мережах електричного зв'язку, комп'ютерним та іншим мереж, шляхом контролю спеціальними технічними засобами і програмним забезпеченням роботи відповідних систем і пристроїв, а також випромінюваних ними електромагнітних та інших полів.

При допиті обвинуваченого в скоєнні інтернет-шахрайства, рекомендується враховувати такі особливості.

- Ефективність допиту багато в чому залежить від того, в якому психологічному стані перебуває допитуваний, від усвідомлення обвинувачуваним в інтернет-шахрайстві своєї провини, від готовності дати правдиві свідчення.

– Оскільки шахраї володіють «живим» розумом, то якщо вони вирішили протидіяти слідству, основною зброєю слідчого повинен стати інтелект, кінцевою метою застосування якого повинно стати викриття допитуваного у брехні, постановка перед єдино можливим виходом - говорити правду.

- При підготовці до допиту і потерпілого і обвинуваченого в інтернет-шахрайстві, при наявності реальної можливості, слідчому рекомендується проконсультуватися з психологом для побудови найбільш ефективної тактики допиту. Також, корисною буде консультація фахівця в сфері високих технологій, результати якої дозволять врахувати специфіку конкретно розслідуваної інтернет-шахрайства.

Потерпілі від шахрайства в мережі Інтернет найчастіше схильні приховувати не тільки окремі факти, що свідчать про скоєний діянні, а й взагалі приховувати свій статус.

Обшук є одним з найскладніших слідчих дій, нарівні з допитом обвинуваченого і підозрюваного. Певні труднощі виникають, в тому числі, і в зв'язку з примусовим характером обшуку, який часом є вторгненням в приватне житло громадян, зачіпає суттєві права й інтереси обшукуваного, іноді - членів його сім'ї, викликає підвищену психологічне навантаження у його учасників. Тому найчастіше його проведення вимагає від співробітників правоохоронних органів певного психологічного напруження, спостережливості, витримки, холоднокровності, такту, особливо щодо членів сім'ї обшукуваного.

Об'єктами пошуку при проведенні обшуку при розслідуванні інтернет-шахрайства можуть бути: а) знаряддя вчинення злочину або їх складові частини (різні ЕОМ і деталі від них і ін.); б) предмети зі слідами вчиненого злочину; в) предмети-результати злочинної діяльності (підроблені документи, фальшиві гроші і т.д.); г) викрадене майно, документи, гроші або цінності; д) сховок шахрая; е) документи, що відображають важливі для справи обставини (записні книжки, квитанції, чеки тощо); ж) майно і цінності, що підлягають вилученню для відшкодування матеріальних збитків або забезпечення можливої конфіскації; з) зразки для порівняльного дослідження; і) предмети, вилучені з цивільного обороту або обмежені в ньому за відсутності спеціального дозволу на володіння ними.

На підготовчій стадії обшуку слідчому рекомендується передбачити, щоб запрошені поняті мали певні пізнання в сфері інформаційних технологій. При проведенні обшуку важливо максимально обмежити обшукувану особу, яка підозрюється в інтернет-шахрайстві, в використанні будь-яких електронних пристроїв, а також виключити вільне пересування обшукуваного і, особливо, несанкціонований доступ до цифрової техніки. В ході проведення обшуку, особливо в заключній стадії, слідчому бажано постійно взаємодіяти з фахівцем, який здійснює допомогу у виявленні слідів злочину, пов'язаних з використанням комп'ютерів, а також консультує членів оперативно-розшукової групи з питань, пов'язаних і інформаційними технологіями, що мають відношення до розслідуваної кримінальної справи.

РОЗДІЛ 3. ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ПРИ РОЗСЛІДУВАННІ ШАХРАЙСТВА В МЕРЕЖІ ІНТЕРНЕТ

3.1. Процесуальні форми використання спеціальних знань

У процесі розслідування злочинів досить часто виникає необхідність вирішення питань, які потребують особливих професійних знань. Це особливо очевидно, з огляду на постійний розвиток високих технологій. У цих умовах, як справедливо зазначає М.Ю. Літвінов, «інститут спеціальних знань становить невід'ємну і дуже важливу частину як практичної діяльності по збиранню, перевірці, і оцінці доказів, так і її кримінально-процесуальні форми» [65, с. 86] .

Брак знань, що виходять за межі професійних юридичних знань слідчих і загальних знань інформаційних технологій, при необхідності заповнюється залученням до розслідування суб'єктів, для яких такі знання є професійними. Подібні знання в кримінально-процесуальному законодавстві іменуються спеціальними. Гідність спеціальних знань полягає в тому, що вони відкривають, по суті, необмежені можливості для достовірного використання досягнень науки і техніки при розслідуванні злочинів в порядку, встановленому законом.

Питанням класифікації форм використання спеціальних знань в науковій літературі приділяється значна увага. Звісно ж, що форми використання спеціальних знань спеціаліста і експерта при розслідуванні, в тому числі інтернет-шахрайства та інших злочинів у сфері високих технологій, повинні базуватися на певних вимогах, в числі яких: норми процесуального права; достовірність, допустимість і належність одержуваної за допомогою експерта або спеціаліста доказової інформації, а також концептуальний рівень розвитку наукових знань і апробовані методики їх використання. Кожна з форм участі спеціаліста або експерта в провадженні у кримінальній справі передбачає використання його спеціальних знань для досягнення цілей кримінального судочинства.

За характером правової регламентації, виявлення і розслідування злочинів у сфері кіберпростору та високих технологій, виділяють дві форми використання спеціальних знань: процесуальні (передбачені кримінально-

процесуальним законодавством) і непроцесуальні форми (прямо не передбачені КПК України).

У зв'язку з цим формами використання спеціальних знань при розслідуванні економічних злочинів в кіберпросторі є наступні:

1. Процесуальні форми використання спеціальних знань:

1) участь спеціаліста в провадженні слідчих дій;

2) участь спеціаліста в судовому розгляді;

3) здійснення судової експертизи і дача висновку спеціаліста, а також показання експерта і свідчення спеціаліста.

2. Непроцесуальні форми використання спеціальних знань:

1) надання досвідченими особами (спеціалістами та експертами) довідково-консультативної допомоги співробітникам правоохоронних органів;

2) участь спеціалістів в оперативно-розшукових заходах;

3) виконання ревізійних і аудиторських перевірок;

4) проведення фахівцем попередніх досліджень матеріальної обстановки місця події і речових доказів під час його участі в слідчих діях.

Серед непроцесуальних форм виділяють також і інші (наприклад, спільний зі співробітниками правоохоронних органів аналіз практики розкриття і розслідування злочинів, підготовці спільних інформаційних та методичних матеріалів, спрямованих на профілактику злочинів та інших правопорушень). Однак необхідно виключити їх зі списку, оскільки вони не відіграють великої ролі в розслідуванні інтернет-шахрайства, їх розгляд в нашому дослідженні буде зайвим.

На думку В. В. Маркова, об'єктивним критерієм розподілу форм використання спеціальних знань на процесуальні і непроцесуальні є характер результату, одержуваного при застосуванні тієї чи іншої форми використання спеціального знання [68, с. 113]. Тобто, якщо результат повинен мати доказове значення, то це об'єктивний показник того, що дану форму використання спеціального знання слід відносити до процесуальних форм.

Тепер необхідно визначити, які знання повинні вважатися спеціальними. Більшість авторів вважає, що «спеціальні» - це, по-перше, знання не

загальновідомі («Не загальновживані», «не повсякденні», «не мають масового поширення»); і, по-друге, не правові.

Глобальна інформатизація, яку зараз переживають багато країн, в тому числі і Україна, безумовно, сильно впливає на критерії, що визначають загальнодоступність, буденність знань. У зв'язку з цим, деякі вчені ставлять справедливе запитання, чи є спеціальними і загальновідомими відомості, викладені в призначених для широкого кола читачів енциклопедіях, довідниках, словниках, представлені в електронних засобах масової інформації, глобальної комп'ютерної мережі Інтернет?

Як зазначає Самойленко О. А., «літературу, присвячену основам і принципам програмування, мережних технологій, влаштуванню засобів комп'ютерної техніки та інших питань комп'ютерних технологій, можна без зусиль знайти, практично в будь-якому книжковому магазині, не кажучи вже про те, скільки інформації з даної тематики викладено в мережі Інтернет » [94, с. 25]. Проте, потрібно відзначити, що наявність навичок досвідченого користувача, які не систематизовані знання в програмуванні і т.п., не можуть служити підставою для притягнення особи в якості спеціаліста.

Деякі вчені виключають зі списку спеціальних знань в кримінальному процесі професійні знання слідчих і суддів, а не правові знання в широкому сенсі. Тобто, в даному випадку, мова йде про те, що в процесі своєї професійної діяльності накопичують певний обсяг знань (наприклад, в сфері бухгалтерії, програмного забезпечення, комп'ютерної техніки і т.д.). Залежно від різних факторів ці знання за своїм змістом можуть в чомусь збігатися з аналогічними знаннями фахівців. І фахівець, і слідчий можуть використовувати ці знання, проте форма використання буде різною [97, с. 236]. Тарасюк А. В. додає ще одну за цілям застосування спеціальних знань [100, с. 184].

Виходячи з вище сказаного, під спеціальними знаннями слід розуміти знання різних сфер науки, техніки, мистецтва і т.д., які не є загальновідомими і загальнодоступними, а також навички їх застосування. З точки зору шахрайства в мережі Інтернет визначення спеціальних знань може бути дано в більш обмеженому вигляді і охоплювати лише пізнання в дуже вузьких рамках, якщо

вони мають поглиблений систематизований характер, наприклад, знання про пристрій і функціонування певного виду комп'ютерної техніки або певних програмних продуктів. Залучаючи фахівців до участі в слідчих діях, призначаючи експертизу, необхідно пам'ятати про предметну спеціалізацію експертів та спеціалістів.

Таким чином, спеціальні знання (з точки зору економічних злочинів у кіберпросторі) - це поглиблені систематизовані знання високих інформаційних технологій і комп'ютерної техніки, доступні вузькому колу спеціалістів, а також практичні навички використання цих знань, вироблені в процесі професійної діяльності.

Як неодноразово зазначалося у нашій роботі, шахрайство в мережі Інтернет відноситься до злочинів у сфері високих технологій, в якій слідчий, як правило, не має досить глибоких знань. І тому без допомоги фахівця він може зробити непоправні помилки в ході огляду технічної апаратури, зняття необхідної інформації та / або її вилучення.

Шахрайство в мережі Інтернет, як і інші злочини, зв'язані з використанням електронних документів, скажімо підробка електронних грошей, часто мають високу ступінь латентності, не залишають видимих слідів і складні з точки зору розкриття і збирання доказової інформації в зв'язку зі складністю об'єктів - носіїв цієї інформації, широким застосуванням засобів віддаленого доступу і рядом інших причин. При розслідуванні по справах про економічну кіберзлочинність участь фахівця в сфері розробки та використання сучасних інформаційних технологій необхідно, оскільки, навіть найменші некваліфіковані дії з комп'ютерною системою можуть привести до втрати цінної розшукової та доказової інформації, а на відновлення цієї інформації може знадобитися багато часу.

Розглянувши загальні питання реалізації інституту спеціальних знань у розслідуванні злочинів, вважаємо за можливе перейти до безпосередньої характеристики кожної форми використання цих знань в при розслідуванні шахрайства в мережі Інтернет.

Отож, участь спеціаліста в слідчих діях розглянемо найперше. КПК України закріплює статус спеціаліста як особи, що бере участь у всіх трьох елементах доказової діяльності: збиранні, перевірці та оцінці отриманих доказів.

Успішність проведення слідчої дії багато в чому залежить від якості і повноти, заздалегідь проведених, підготовчих заходів, при яких важливе значення мають:

1) отримання орієнтуючої інформації про особу підозрюваного в інтернет-шахрайстві, про місце проведення дій і можливі джерела доказів;

2) визначення часу, місця і умов його проведення;

3) визначення кола учасників, засобів криміналістичної та комп'ютерної техніки, особливо, вибір фахівця необхідного профілю і кваліфікації.

Спеціалістом визнається особа, яка володіє сучасними науковими, технічними та іншими знаннями, професійним досвідом в певній діяльності, навичками і вміннями використання науково-технічних засобів, запрошених органом дізнання, слідчим, прокурором і судом для участі в слідчих діях чи судовому розгляді і надання сприяння в збиранні, дослідженні та оцінці доказів.

Спеціаліст залучається до проведення слідчих дій для більш правильного з'ясування питань використання певних комп'ютерних засобів в кожній конкретній слідчій ситуації, надання допомоги слідчому в підборі понятих, в якості яких слід залучати осіб, які знаються на комп'ютерній техніці, а також застосовує ці комп'ютерні засоби для виявлення, фіксації та вилучення інформації про вчинений інтернет-шахрайстві [112, с. 124].

Залучаючи фахівців до участі в слідчих діях або призначаючи експертизу, слідчий повинен пам'ятати про предметну спеціалізацію експертів та фахівців. Наприклад, Шеломенцев В. П. вказує, що в залежності від призначення об'єктів, що оглядаються до участі у слідчій дії повинні залучатися такі спеціалісти:

1) з обслуговування і ремонту СВТ (для огляду його апаратної частини і сполучної арматури, наприклад, для ЕОМ - інженер-системотехнік);

2) в сфері мережевих технологій (для огляду СВТ, використовуваних в системах дистанційної передачі даних - мережах ЕОМ і електрозв'язку, периферійного обладнання віддаленого доступу);

3) за відповідним видом електрозв'язку (для огляду обладнання електрозв'язку, використовуваного для передачі комп'ютерних даних і команд; терміналу, який є апаратом електрозв'язку; електронних документів, що містяться в пам'яті апарату електрозв'язку);

4) оператор СВТ - ЕОМ, стільникового радіотелефону, контрольно-касового пристрою, сервера мережі ЕОМ

5) технічний спеціаліст реєстраційного відділу або інший співробітник податкової інспекції (для огляду, вивчення і вилучення електронних документів, що містяться у фіскальній пам'яті касової ЕОМ);

6) інспектор огляду засобів захисту терміналу і поміщеної на ньому комп'ютерної інформації від несанкціонованого доступу, витоку і знімання, а також виявлених спеціальних технічних засобів для негласного отримання (знищення, модифікації, копіювання, блокування інформації);

7) інженер-програміст (для огляду програмного забезпечення, визначення принципу його функціонування, усунення слідів злочинної діяльності в середовищі машинної інформації, надання сприяння в огляді, вивченні і вилучення електронних документів) [115].

Слід погодитися з Шеломенцевим В. П. Говорячи про шахрайство в мережі Інтернет, завжди потрібно мати на увазі, що даний злочин складний і багатогранний. Для досягнення своїх злочинних цілей шахраї використовують різні засоби і їх комбінації. Тому для слідчого надзвичайно важливим є правильний вибір спеціаліста.

Число слідчих дій, при проведенні яких використання спеціальних знань в сфері комп'ютерних технологій при розслідуванні інтернет-шахрайств, неоднакове. Також різні рівень і глибина їх застосування. При розслідуванні шахрайства в мережі Інтернет участь спеціаліста може знадобитися практично на всіх стадіях розслідування, починаючи зі стадії порушення (для отримання достатніх даних, що вказують на ознаки злочину) і закінчуючи розглядом справи в суді (наприклад, для роз'яснення значення зроблених експертом висновків). А при розслідуванні злочинів, сполучених з використанням засобів

комп'ютерної техніки, потреби в допомозі спеціаліста носять більш обмежений характер.

Наприклад, в тих випадках, коли виникає необхідність встановлення факту перебування певних даних на машинному носії інформації, призначення і проведення судової експертизи необов'язково [113, с. 99]. Факт знаходження конкретних даних, що мають значення для кримінальної справи, може бути зафіксований проведенням слідчого огляду з участю спеціаліста. Слід зазначити, що при даній слідчій дії участь спеціаліста і знаючих понятих необхідно, щоб виключити можливі згодом заяви зацікавлених осіб щодо змін, або про можливе внесення інших даних слідчим в ході огляду даних, що містяться в комп'ютерній системі, на машинних носіях інформації.

Для участі в огляді спеціаліста доцільно залучати в тих випадках, коли вивчення самого об'єкта, змін в ньому, пов'язаних з вчиненням інтернет-шахрайства, а також виявлення та фіксація слідів і речових доказів вимагають застосування яких знань, умінь, якими слідчий не має, або технічних засобів, в користуванні якими слідчий не має належних навичок або застосування яких в процесі огляду відверне слідчого від виконання інших, не менш важливих і невідкладних дій при огляді [109, с. 10].

Проведення експертизи. Основною процесуальної формою використання спеціальних знань при розслідуванні та судовому розгляді кримінальних справ є судова експертиза. Вона являє собою призначуване і здійснюване з дотриманням встановлених кримінально-процесуальним законом норм дослідження, на основі застосування спеціальних знань в науці, техніці, мистецтві чи ремеслі і виданні висновку, який має доказове значення. Основний зміст експертизи в кримінальному судочинстві становить аналіз певних даних з метою встановлення нових фактів, що мають значення для досудового розслідування злочинів або розгляду кримінальних справ у суді.

Вид судових експертиз, при виробництві яких використовуються спеціальні пізнання в сфері комп'ютерної техніки та інформаційних технологій, почав формуватися приблизно з середини 1990-х років, шляхом проведення окремих унікальних експертиз. Виникнення нового виду судових експертиз,

пов'язаних з дослідженням комп'ютерних засобів, і початок роботи з його освоєння були обумовлені зростаючими потребами слідчої практики.

На початковому етапі розвитку цього виду експертиз деякими авторами виділялися два види:

1) технічна експертиза комп'ютерів і їх комплектуючих, мета якої - вивчення конструктивних особливостей і стану комп'ютера, його периферійних пристроїв, магнітних носіїв і т.д., комп'ютерних мереж, а також причин виникнення збоїв в роботі вищевказаного обладнання;

2) експертиза даних і програмного забезпечення, що здійснюється з метою вивчення інформації, що зберігається в комп'ютері і на інших носіях [96].

Однак найбільшого поширення набула класифікація комп'ютерно-технічної експертизи, запропонована Струковою В. Є., як виділяє 4 її види:

1) апаратно-комп'ютерна експертиза;

2) програмно-технічна експертиза;

3) інформаційно-комп'ютерна експертиза (даних);

4) комп'ютерно-мережева експертиза [97, с. 236].

У науковій літературі вказується, що дана класифікація прийнята за основу при описі судових експертиз, що призначаються для дослідження засобів комп'ютерної техніки та інформації, більшістю авторів, що займаються дослідженням проблем боротьби зі злочинністю в сфері комп'ютерної інформації.

Для розгляду питань проведення комп'ютерно-технічної експертизи у справах про шахрайство в мережі Інтернет вважаємо за доцільне спиратися саме на вказану класифікацію.

В даний час, для залучення інтернет-шахраїв до кримінальної відповідальності, необхідно застосовувати ч. 3 ст.200 КК України. У зв'язку з цим логічно і допустимо говорити, що призначення і проведення експертиз у справах про шахрайство в мережі Інтернет, в більшості своїй, має ті ж особливості, що і в справах про злочини у сфері комп'ютерної інформації , які передбачені розділом 16 КК України.

Звісно ж, що шахрайство, скоєне тільки з використанням мережі Інтернет - явище нечасте. Злочинцеві не вигідно подібне самообмеження, а тому використовуються і інші засоби, наприклад стільниковий зв'язок або приховані відеокамери, замасковані під конструктивну частину банкомату, що записують РПЧ-коди, що вводяться користувачами. У зв'язку з цим логічно говорити про те, що під час розслідування шахрайства в мережі Інтернет проведення комп'ютерно-технічних експертиз можливе стосовно безлічі різних об'єктів. Практика показує, що всі 4 основних види комп'ютерно-технічної експертизи при проведенні більшості експертних досліджень застосовуються комплексно і, найчастіше, послідовно. Тому в постанові про проведення судової експертизи доцільно вказувати видое найменування експертизи. У цьому випадку керівник експертної установи, ознайомившись з постановою, зможе призначити для проведення експертизи експертів, що володіють найбільш придатною спеціалізацією. В іншому випадку може скластися ситуація, коли частина питань слідчого залишиться без відповіді, через це необхідно буде призначати нову експертизу, що затягне досудове розслідування.

Удосконалення методів боротьби зі злочинністю у сфері високих технологій взагалі та інтернет-шахрайством, зокрема, вимагає від правоохоронних органів більш тісного використання в своїй практиці досягнень науки і техніки. Проведення представниками різних сфер знання спільного дослідження і оцінка виявлених ознак дозволяють конкретизувати відповіді на поставлені питання більшою мірою, ніж самостійні дослідження тих же ознак, здійснені кожним експертом окремо.

Особливість комплексного дослідження полягає в тому, що загальним для експертів виступає мета дослідження, а способи досягнення результатів можуть бути різними. Основне призначення комплексної експертизи - вирішення питань, що відносяться до прикордонних знань експертів, коли досягаються поліаспектні (цілісні) уявлення про досліджуваний об'єкт.

При призначенні експертизи слідчий повинен уявляти собі рівень розвитку сучасної науки, техніки, види експертиз, які можна призначити при

розслідуванні даного шахрайства, а також усвідомлювати можливості тої експертної установи, куди буде направлено постанову.

При здійсненні комп’ютерно-технічної експертизи комп'ютера або іншого пристрою підозрюваного, або обвинуваченого у вчиненні інтернет-шахрайства, в залежності від конкретного виду експертизи, проводиться дослідження наступних об'єктів:

1) Апаратні об'єкти:

a. комп'ютери;

b. комплектуючі для комп'ютерів і інших пристроїв;

c. периферичні пристрої (принтери, сканери, модеми та т.д.);

d. мережеві апаратні засоби (сервери, мережеві кабелі і т.д.);

e. інтегровані системи (мобільні телефони, органайзери та ін.).

2) Програмні об'єкти:

a. системне програмне забезпечення;

b. прикладне програмне забезпечення.

3) Інформаційні об'єкти (дані):

a. документи, виготовлені за допомогою комп'ютерних засобів;

b. дані в мультимедійні форматах (аудіо- та відеофайли, зображення і т.д.)

c. комп'ютерна інформація, що міститься в базах даних [5, с. 194].

Іншої класифікації дотримуються зарубіжні криміналісти. Зокрема, І. Кейсі пропонує таку класифікацію об'єктів-джерел криміналістично значимої інформації:

1. Комп'ютери. Дану групу утворюють:

a. стаціонарні комп'ютери під управлінням операційних систем Windows, Unix і Macintosh (Mac OS X);

b. портативні пристрої.

2. Комп'ютерна мережа (за рівнями взаємодії комп'ютерних систем):

a. фізичний рівень;

b. мережевий рівень;

c. транспортний рівень;

d. сеансовий рівень;

e. рівень представлення даних;

f. прикладний рівень [19].

Не вдаючись в подробиці аналізу кожного об'єкта, відзначимо, що дана класифікація має свої переваги і недоліки в порівнянні з класифікацією об'єктів, запропонованої вище. З одного боку, класифікація І. Кейсі враховує положення міжнародного стандарту OSI (взаємодії відкритих систем), що полегшує класифікацію видобутої в процесі розслідування інформації про злочинну діяльність інтернет-шахраїв, а також її подальше вивчення. З іншого боку, поділ об'єктів експертизи на апаратні, програмні та інформаційні, на наш погляд, є більш підходящим для національних експертів з точки зору криміналістики.

Напрямок та обсяг експертного дослідження визначаються питаннями, поставленими слідчим перед експертом. Конкретне формулювання питання повинно залежати від можливостей науки і техніки, складу злочину, що розслідується, компетенції експерта.

Таким чином, питання, які слідчий ставить перед експертом при призначенні комп'ютерно-технічної експертизи, можна згрупувати за ознакою об'єкта, що направляється на дослідження.

Результати експертизи оформляються у письмовому вигляді у формі мотивованого висновку експерта з докладним викладом всіх матеріалів дослідження. У тих випадках, коли експерт встановив обставини, що мають, з його точки зору, значення для справи, але не знайшли відображення в постанові про призначення експертизи, він зобов'язаний повідомити про це слідчому.

Незважаючи на особливий статус експертизи як професійного дослідження, висновок експерта не є доказом за замовчуванням, оскільки слідчий, оцінивши результати експертизи, має право не враховувати їх в подальшому ході розслідування [24, с. 27]. У цьому зв'язку доречно навести слова І. О. Громико про оцінку слідчим висновку експерта: «неприпустимо ... оцінювати висновок експерта тільки як висновок, відкидаючи мотивування і аргументацію цього висновку, виявлені в процесі дослідження фактичні дані і весь хід дослідження.

Висновок експерта має значення лише остільки, оскільки він обґрунтований фактичними даними » [29, с.37].

При розслідуванні шахрайства в мережі Інтернет і інших комп'ютерних злочинів не завжди існує можливість провести експертне дослідження в лабораторії, наприклад, якщо стало відомо, що комп'ютер шахрая має високу ступінь захисту або цей комп'ютер є важливою складовою корпоративної мережі компанії і його вилучення неможливо без заподіяння істотної шкоди цій компанії.

Використання при огляді місця події або проведенні обшуку спеціальних знань у формі судових експертиз обумовлено діяльністю експерта по дослідженню наданих йому матеріалів з метою виявлення доказів. Цей період роботи експерта ділиться на два етапи:

1) діяльність судового експерта безпосередньо на місці події, пов'язаного з інтернет-шахрайством;

2) дослідження отриманих матеріалів в експертній установі.

Дослідження, що проводяться на місці події, в криміналістиці отримали назву ситуаційної експертизи [40, с. 99]. Незважаючи на оригінальність назви, ситуаційна експертиза не є самостійним або особливим видом судової експертизи, а, скоріше, додаткової стадією експертизи. При проведенні ситуаційної комп'ютерно-технічної експертизи в будівлі, де розташовується юридична особа, працівником якого є обвинувачуваний в інтернет-шахрайстві, слідчому необхідно забезпечити експерту максимальний доступ до необхідної інформації. Якщо мова йде про великій фірми, то, цілком можливо, що в ній існує служба або департамент інформаційної безпеки в складі служби загальної безпеки. Такий підрозділ за замовчуванням володіє майже всією інформацією про інформаційно-комп'ютерні ресурси компанії і, при необхідності, зможе максимально спростити роботу експерту, наприклад з клонуванням жорстких дисків комп'ютера інтернет-шахрая для подальшого вивчення їх вмісту в лабораторних умовах.

Участь обізнаних осіб у судовому розгляді. Як і на стадії попереднього розслідування, під час судового розгляду може виникнути необхідність в

залученні до участі обізнаних осіб для роз'яснення різних питань. Це особливо актуально, якщо мова йде про злочини в сфері високих технологій, і особливо, про шахрайство в мережі Інтернет.

В ході розгляду кримінальної справи в суді завданням спеціаліста є роз'яснення питань щодо матеріалів справи, що входять в його компетенцію. Слід пам'ятати, що фахівець, який брав участь в попередньому розслідуванні, по суті, подібний до свідка, а тому - є додатковим джерелом цінної для слідства інформації, що дозволяє залучити інтернет-шахрая до кримінальної відповідальності.

В процесі розгляду справи про шахрайство в суді спеціаліст може надати наступну інформацію:

1) про оперативно-розшукові заходи та слідчі дії, в яких він брав участь;

2) відомості довідково-інформаційного характеру (наприклад, про функції певного пристрою, вилученого під час обшуку у інтернет-шахрая);

3) проконсультувати по загальних і особливих питаннях (наприклад, про принципи роботи корпоративних локальних комп'ютерних мереж) з метою правильного розуміння судом і іншими учасниками судового засідання всіх матеріалів кримінальної справи про інтернет-шахрайство.

Ряд авторів виділяють ще одну процесуальну форму використання спеціальних знань - це самостійне, без сприяння обізнаних осіб, використання слідчим спеціальних знань. Наприклад, Карчевський М. В. до процесуальних форм відносить безпосереднє використання їх слідчим, і судом при виконанні своїх процесуальних функцій збирання, дослідження і оцінки доказів [42, с. 15]. Звісно ж, що при розслідуванні шахрайства в мережі Інтернет така форма використання спеціальних знань малозастосовна. Слідчий, що володіє спеціальними знаннями в сфері користування комп'ютерами, може самостійно, без залучення фахівців оглянути персонального комп'ютера, але висока ймовірність того, що підозрюваний користується програмними засобами захисту інформації і при спробі перегляду важлива інформація буде знищена, або для отримання доступу потрібно залучення знань в сфері криптографії та

шифрування, використання навичок зняття парольного захисту, якщо підозрюваний відмовляється добровільно назвати необхідний код.

Треба пам’ятати, що навіть якщо підозрюваний йде на співпрацю і добровільно дає всі необхідні паролі для забезпечення доступу, слід мати на увазі, що існують програми, які, при введенні неправильного або певного коду, знищують інформацію. Також слід враховувати те, що підозрюваний може включити до складу програмного забезпечення свого комп'ютера такі програми, які будуть періодично запитувати пароль, і, якщо протягом декількох секунд правильний пароль не введений, важливі для розслідування інтернет-шахрайства дані будуть автоматично знищені або заблоковані [42].

Зарубіжні дослідники проблем розслідування комп'ютерних злочинів відзначають, що слідчі повинні вміти поводитися з комп'ютерами, не завдаючи шкоди матеріальним цінностям, засобам до існування і правам свідків і підозрюваних користувачів при розслідуванні комп'ютерного злочину і як важливі відповідні навички і знання для проведення ефективного розслідування. У зв'язку з цим представляється необхідним відзначити наступні факти:

1) шахрайство в мережі Інтернет, як правило, відбувається особами, що мають глибокі пізнання в сферы комп'ютерних технологій;

2) для ефективного виявлення і закріплення слідів злочину потрібні відповідні знання та навички, які не поступаються використаним злочинцем;

3) при сучасних темпах розвитку комп'ютерної техніки знання слідчого в цій сфері, з об'єктивних причин, не можуть завжди відповідати вимогам, необхідним для успішного проведення слідчих дій без допомоги обізнаних осіб.

Виходячи зі сказаного, можна зробити висновок, що власні знання слідчого в сфері високих технологій в більшості випадків виявляться недостатніми для самостійного дослідження комп'ютерної техніки. Більш того, навіть якщо слідчий володіє необхідними спеціальними знаннями, що може бути обумовлено його попередньою професією, наявністю відповідного диплома, сертифікатів і т.п., необхідно залучення експерта або спеціаліста для надання висновку.

Наявність у слідчого необхідних знань в сфері комп'ютерних технологій може бути застосовано при висуненні версій, плануванні та організації розслідування злочинів, знаходженні доказів і їх оцінці. Однак, інформація, що містить відомості спеціального характеру і отримана з непроцесуальних джерел (яким в даному випадку буде слідчий), служить лише приводом для прийняття рішення про використання знань обізнаних осіб в формах, встановлених кримінально-процесуальним законодавством. З огляду на те, що комп'ютерні технології досить різноманітні, наявність подібних знань у слідчого буде корисно для правильного визначення кола фахівців, чиї знання потрібні для вирішення конкретних питань. Оскільки кримінально-процесуальний закон забороняє суміщення в одній і тій же особі кількох процесуальних ролей, то слідчий не зможе виконувати одночасно, наприклад, роль слідчого і експерта або спеціаліста. Тому навіть якщо слідчий володіє дипломами та сертифікатами, що підтверджують його кваліфікацію та рівень знань в сфері високих технологій, його участь в якості обізнаної особи при провадженні слідчих дій у справах про інтернет-шахрайство має виключати його роль як слідчого. Проте, в деяких випадках представляється обґрунтовано вважати допустимим самостійне застосування спеціальних знань в сфері високих технологій.

3.2 Непроцесуальні форми використання спеціальних знань

Як зазначається в науковій літературі, непроцесуальна форма застосування спеціальних знань в розслідуванні злочинів не регулюється нормами КПК України, а здійснюється або відповідно до відомчих інструкцій, або на розсуд слідчого (звідси і назва форми) [46, с. 77].

Непроцесуальне використання спеціальних знань включає в себе виконання таких функцій:

1) консультації слідчого з питань, що потребують спеціальних знань;

2) складання різних довідок за дорученням слідчого (довідкова діяльність обізнаної особи);

3) використання результатів позасудових (відомчих, адміністративних) досліджень (розслідувань), що проводяться спеціальними комісіями;

4) надання технічної допомоги слідчому (наприклад, допомога в установці відслідковуючого програмного забезпечення на комп'ютер підозрюваного в інтернет-шахрайстві);

5) використання результатів перевірок, проведених працівниками різних відомств і інспекцій;

6) використання матеріалів попереднього (позасудового) експертного дослідження різних об'єктів (наприклад, речові докази) [51, с. 99].

Всі наведені вище функції можна об'єднати в три основні форми непроцесуального використання спеціальних знань, які можна застосувати в розслідуванні економічної злочинності вкіберпросторі: участь спеціаліста в оперативно-розшукових заходах, надання довідково-інформаційної допомоги слідчому і консультаційна діяльність. Розглянемо кожну з цих форм докладніше.

Участь фахівця в оперативно-розшуковому заході. Як показує практика розслідування, особливі проблеми процесуального та психологічного плану слідчі зустрічають при провадженні окремих слідчих дій, в ході яких необхідно провести виявлення, фіксацію і вилучення комп'ютерної інформації.

Головне завдання спеціаліста при здійснені оперативно-розшукового заходу - допомогти слідчому отримати максимум інформації, необхідної для успішного розслідування шахрайства в мережі Інтернет.

Спеціаліст також може залучатися до проведення оперативно-розшукових заходів для з'ясування питань використання певних комп'ютерних чи інших засобів в конкретній слідчій ситуації, надання допомоги слідчому в підборі понятих, в якості яких рекомендується залучати осіб, які знаються на комп'ютерній техніці.

При здійсненні такого оперативно-розшукового заходу як зняття інформації з технічних каналів зв'язку, спеціаліст повинен підібрати необхідне обладнання і програмне забезпечення, при використанні яких у підозрюваного

інтернет-шахрая не виникне підозр про що ведеться стосовно нього розслідування.

Взагалі, тактика пошуку інформації в комп'ютері інтернет- шахрая під час проведення будь-яких оперативно-розшукових заходів і слідчих дій полягає в правильному застосуванні криміналістичних прийомів її виявлення. Знання цих прийомів дозволить слідчому:

1) не допустити знищення або пошкодження отримуваної інформації;

2) правильно розібратися в складному інформаційному масиві і знайти необхідну;

3) правильно зафіксувати вилучену інформацію в криміналістичному і процесуальному плані.

Слід заздалегідь заручитися допомогою відповідних спеціалістів, особливо якщо є підстави вважати, що підозрюваний у шахрайстві використовує комп'ютер як сховище і інструмент обробки інформації про злочинну діяльність, наприклад інформації про викрадені за допомогою шкідливої програми особистих даних користувачів платіжної системи, відомостей про протиправні оборудки і їх зміст , іншої інформації, що становить інтерес для слідства.

Залучення спеціаліста в сфері комп'ютерних технологій може знадобитися не тільки при організації та проведенні обшуку, виїмки, експертного дослідження отриманих матеріалів, а й для надання допомоги слідчому при проведенні допитів, очних ставок тощо.

Звісно ж необхідно зазначити, що залучені досвідчені особи (якщо це не співробітники відомчих експертних підрозділів, які мають необхідний досвід), як правило, не володіють правовими знаннями, що нерідко стає причиною процесуальних порушень. У зв'язку з цим, слідчому необхідно загострити увагу на детальному роз'ясненні прав і обов'язків спеціаліста перед початком слідчої дії.

Довідково-інформаційна та консультативна допомога фахівця дає можливість слідчому правильно орієнтуватися в обстановці, що склалася, приймати рішення про призначення певної експертизи, визначати коло питань, адресованих експертові, і т.д. Сутність такої форми використання спеціальних

знань - постановка письмових запитань слідчого спеціалісту, який дає відповідь у вигляді довідки, не проводячи спеціального дослідження. Відмінністю довідкової допомоги спеціаліста є відсутність необхідності проводити дослідження, в іншому випадку мова буде йти про експертизу.

Видача довідок передбачає використання інформації:

1) яка міститься в картотеках (наприклад, картотеках шкідливих програм) і колекціях;

2) знаходиться в будь-якій галузі знання;

3) отриманої шляхом умовиводів фахівців однієї або декількох галузей знань.

Консультації осіб, які мають спеціальну підготовку, не є висновком про будь-які обставини вчиненого злочину, проте допомагають слідчому отримати деяку попередню, важливу для розслідування, інформацію.

Фахівцем-консультантом є особа, яка має спеціальні знання, професійний досвід в певній діяльності, навички, вміння використовувати науково-технічні засоби і спеціальні знання і на прохання слідчого, органу дізнання, прокурора і суду пояснює сутність предметів, явищ, що показує ефективні напрямки застосування досягнень науково -технічного прогресу [55, с. 420].

Звісно ж, що консультаційну діяльність фахівця можна реалізувати практично на всіх етапах досудового розслідування і розгляду кримінальної справи про інтернет-шахрайство в суді. Розглянемо особливості консультаційної діяльності на деяких етапах досудового розслідування.

Консультаційна діяльність спеціаліста включає, перш за все, сприяння слідчому у вирішенні тактичних питань, тобто надання допомоги у виробленні слідчих версій, складанні планів розслідування або проведенні окремих слідчих дій і т.п. У вирішенні цих питань фахівець може надати слідчому істотну допомогу. Така допомога, що надається слідчому з питань, пов'язаних з розслідуванням інтернет-шахрайства, в процесуальних документах не завжди знаходить своє відображення. Вона може полягати в повідомленні слідчому спеціальних відомостей з сфер науки, техніки, необхідних при розслідуванні злочину.

При призначенні експертизи, слідчому рекомендується проконсультуватися з спеалістом (або навіть з експертом, який буде проводити експертизу), щоб скласти найбільш грамотну постанову. У зв'язку з цим завдання спеціаліста зводиться до допомоги слідчому у відповіді на такі питання як:

1. Який конкретно вид експертизи призначити?

2. Які саме об'єкти необхідно дослідити?

3. Які питання повинні бути поставлені перед експертом в обов'язковому порядку?

Звісно ж, що така консультація буде особливо необхідна, якщо мова йде про призначення авторознавчої експертизи комп'ютерних програм або матеріалів, отриманих, наприклад, при дослідженні інтернет-сайту, створеного злочинцем для здійснення Інтернет-шахрайства, оскільки дослідження подібних об'єктів (особливо комп'ютерних програм) являє собою складний процес, що вимагає великих витрат часу і сил.

Також в ході підготовки до слідчої дії (наприклад, обшуку приміщення, де працює інтернет-шахрай) або при його проведенні, спеціаліст консультує учасників з питань, пов'язаних з поводженням з технічними пристроями, функціями програмного забезпечення і т.д. При необхідності, спеціаліст роз'яснює питання, пов'язані з використанням спеціальних технічних засобів, призначених для виявлення, вилучення і фіксації інформації, що має значення для розслідування шахрайства в мережі Інтернет.

В юридичній літературі справедливо піднімається питання про те, чи існує можливість процесуально оформити консультацію спеціаліста, за допомогою якої він допомагає слідчому сформулювати питання перед експертом. Звісно ж, що в більшості досліджень, присвячених цій проблемі, лише констатується її наявність, але не пропонується нічого конкретного для її рішення. В якості одного з варіантів оформлення такої консультації можна скористатися викликом спеціаліста для допиту і зафіксувати його рекомендації щодо формулювання питань експерту в протоколі допиту, що може мати місце в тих випадках, коли порушене кримінальне провадження. З одного боку, така міра

загрожує перевантаженням кримінальної справи документами, але з іншого - не суперечить кримінально-процесуальному закону.

Однак, на наше переконання, при розслідуванні економічних кіберзлочинів, як і інших комп'ютерних злочинів, переведення консультації спеціаліста в процесуальну форму не зіграє істотної ролі: консультацію цілком можна провести неформально, а потім, при складанні постанови про призначення експертизи, врахувати рекомендації, дані спеціалістом. В іншому випадку може скластися ситуація, коли кримінальна справа про інтернет-шахрайство буде перевантажено зайвими для розслідування документами.

Як зазначається в юридичній літературі, використання результатів відомчого розслідування є однією з поширених форм непроцесуального застосування спеціальних знань [56, с. 65]. Недооцінка важливості проведення технічної інспекції, яку складено за результатами внутрішньовідомчого розслідування, призводить до призначення судово-технічних експертиз по досить очевидних справах, в яких є кваліфіковані висновки. Проведення зайвих або необґрунтовано ємних експертиз затягує розслідування інтернет-шахрайства, що знижує ефективність залучення до відповідальності винних. Вважаємо за необхідне, однак, вказати, що документи, що фіксують результати внутрішньовідомчого розслідування, не можуть прирівнюватися до висновку експерта і служити підставою для відмови в проведенні експертизи.

З точки зору юридичної особи, інтернет-шахрайство, як і інші злочини в сфері високих інформаційних технологій, є інцидентом інформаційної безпеки, оскільки, незважаючи на кінцеву мету шахрайства - викрасти обманним шляхом цінне майно, основна суть цього злочину одна - це порушення цілісності інформаційної безпеки організації.

Виходячи зі змісту стандартів інформаційної безпеки 180 / 1ЕС 27000, загальна схема організації процесу реагування на інцидент шахрайського характеру ґрунтується на постановці кількох кінцевих цілей:

1) відновлення нормальної працездатності підприємства в найкоротші терміни;

2) підтвердження або спростування факту інциденту;

3) уявлення детального звіту про інцидент і рекомендацій. Створення умов для накопичення і зберігання точної інформації про комп'ютерні інциденти, які мали місце, забезпечення швидкого виявлення та / або попередження подібних інцидентів в майбутньому;

4) забезпечення збереження і цілісності доказів інциденту, створення умов для порушення цивільної або кримінальної справи проти зловмисника;

5) мінімізація порушення порядку роботи і пошкодження даних інформаційної системи, мінімізація наслідків порушення конфіденційності, цілісності та доступності інформаційної системи;

6) захист репутації компанії і її ресурсів;

7) проведення навчання співробітників компанії про процес реагування на інцидент [59].

Як видно, цілі відомчого розслідування Інтернет-шахрайства, яке порушило цілісність системи інформаційної безпеки організації, багато в чому схожі з цілями розслідування такого правоохоронними органами. У зв'язку з цим можна зробити наступний висновок: інформація, отримана в ході відомчого розслідування за фактом вчинення і Інтернет-шахрайства, може мати доказове значення для слідчого і суду.

Оскільки відомче розслідування інцидентів інформаційної безпеки, в числі яких і інтернет-шахрайство, має на увазі обов'язкове залучення спеціалістів з різних сфер (відділ кадрів, юристи, технічні експерти, зовнішні консультанти з інформаційної безпеки, бізнес-менеджери, співробітники служб технічної підтримки, співробітники служби безпеки), отримані в результаті такого розслідування дані можуть істотно полегшити роботу слідчого. Наприклад, за результатами відомчого розслідування може бути отримана інформація:

1) яка вказує на використання шкідливого програмного забезпечення і подробиці його поширення;

2) більш детально характеризує спосіб і механізм вчинення злочину;

3) має відношення до осіб, які вчинили посягання (реальний IP-адреса віддаленого комп'ютера, конкретний комп'ютер всередині компанії і т.д.) ;

4) точніше характеризує предмет посягання інтернет- шахраїв (ідентифікаційні і кількісні характеристики майна, а також його вартість) і ін. [63].

Таким чином, результати відомчого розслідування факту інтернет-шахрайства можуть використовуватися слідчим при проведенні слідчих дій та призначення судових експертиз. Зокрема, така інформація дозволить: по-перше, формулювати конкретніші питання і завдання експерту при підготовці постанови про призначення експертизи; по-друге, більш чітко уявляти собі загальну картину злочину, з меншими труднощами підбирати фахівців для кожної слідчої дії; по-третє, виявити і розшукати спільників інтернет-шахрая, якщо вони були.

Для розслідування шахрайства в мережі Інтернет становить інтерес і така непроцесуальна форма використання спеціальних знань, як попереднє дослідження об'єктів, зокрема, в роботі з речовими доказами.

Попередні дослідження слідів злочину як вид непроцесуальної діяльності обізнаних осіб, полягають в проведенні досліджень в лабораторних умовах співробітниками експертних установ по складах злочинів:

1) де питання про наявність в діях особи, що перевіряється ознак кримінально караного діяння потребує вирішення на основі застосування спеціальних знань, а також коли

2) з метою пошуку злочинця по гарячих слідах виникає необхідність позапроцесуального оперативного застосування спеціальних знань для вирішення простих діагностичних і ідентифікаційних завдань.

Попереднє дослідження дозволяє більш ефективно здійснювати відбір об'єктів для подальшого порівняльного дослідження; оперативно перевірити значну кількість документів в реальній і електронній формі, речових об'єктів; прочитати закреслений, розмитий текст; встановити, чи виконаний текст на одному комп'ютері або на різних; визначити, чи виконаний відбиток печатки (штампа) фабричним або кустарним способом або відсканований, і інші обставини, важливі для вирішення питання про порушення кримінального провадженя. Інформація, отримана в ході попереднього дослідження, дозволяє:

1) отримати більш чітке уявлення про масштаб діяльності інтернет-шахрая;

2) визначити конкретні способи вчинення злочину;

3) організувати розшук шахраїв;

4) виявити ознаки інших злочинів, вжити інших заходів щодо розкриття шахрайства та виявлення злочинця.

При проведенні попереднього дослідження спеціаліст використовує такі методи, які виключають знищення або зміну первісного вигляду і властивостей речового доказу. При цьому трапляються можливими випадки, коли фахівець, маючи в своєму розпорядженні клонкопію жорсткого диска підозрюваного інтернет-шахрая, може отримати доступ до втраченої під час обшуку комп'ютерної інформації за рахунок застосування спеціальних програмних засобів. У цьому випадку слідчий зможе використовувати цю інформацію, наприклад, при допиті підозрюваного, оскільки останній, можливо, буде впевнений в тому, що дана інформація знищена.

Висновок до розділу 3.

Підводячи підсумок дослідженню використання спеціальних знань при розслідуванні інтернет-шахрайства, можна зробити наступні висновки.

За характером правової регламентації, виявлення і розслідування злочинів у сфері комп'ютерної інформації та високих технологій, виділяють наступні форми використання спеціальних знань:

1. Процесуальні форми використання спеціальних знань:

1) участь спеціаліста в провадженні слідчих дій;

2) участь спеціаліста в судовому розгляді

3) проведенні судової експертизи і подання висновку спеціаліста, а також показання експерта і свідчення спеціаліста.

2. Непроцесуальні форми використання спеціальних знань:

1) надання досвідченими особами (спеціалістами та експертами) довідково-консультативної допомоги співробітникам правоохоронних органів;

2) участі спеціалістів в оперативно-розшукових заходах;

3) виконання ревізійних і аудиторських перевірок;

4) проведення фахівцем попередніх досліджень матеріальної обстановки місця події і речових доказів під час його участі в слідчих діях.

Залучаючи спеціалістів до участі в слідчих діях або призначаючи експертизу, слідчий повинен пам'ятати про предметну спеціалізацію експертів та спеціалістів.

При розслідуванні шахрайства в мережі Інтернет участь спеціаліста може знадобитися практично на всіх стадіях розслідування, починаючи зі стадії порушення (для отримання достатніх даних, що вказують на ознаки злочину) і закінчуючи розглядом справи в суді (наприклад, для роз'яснення значення зроблених експертом висновків).

При розслідуванні шахрайства в мережі Інтернет і інших комп'ютерних злочинів не завжди існує можливість провести експертне дослідження в лабораторії, наприклад, якщо стало відомо, що комп'ютер шахрая має високу ступінь захисту або цей комп'ютер є важливою складовою корпоративної мережі компанії і його вилучення неможливо без заподіяння істотної шкоди цій компанії.

У процесі розгляду справи про шахрайство в суді спеціаліст може надати наступну інформацію:

1) про оперативно-розшукові заходи та слідчі дії, в яких він брав участь;

2) відомості довідково-інформаційного характеру;

3) проконсультувати по загальних і особливих питаннях з метою правильного розуміння судом і іншими учасниками судового засідання всіх матеріалів кримінального провадження.

Власні знання слідчого в сфері високих технологій в більшості випадків можуть виявитися недостатніми для самостійного дослідження комп'ютерної техніки. Навіть якщо слідчий володіє необхідними спеціальними знаннями, що може бути обумовлено його попередньою професією, наявністю відповідного диплома, сертифікатів і т.п., необхідно залучення експерта або спеціаліста для надання висновку.

Непроцесуальна форма застосування спеціальних знань в розслідуванні злочинів не регулюється нормами КПК, а здійснюється або відповідно до відомчих інструкцій, або на розсуд слідчого. Консультаційна діяльність фахівця включає, перш за все, сприяння слідчому у вирішенні тактичних питань, тобто надання допомоги у виробленні слідчих версій, складанні планів розслідування або виробництва окремих слідчих дій і т.п.

ВИСНОВОК

Проведене в даній роботі дослідження дозволяє зробити певні висновки, відповідні пропозиції і рекомендації.

У процесі дослідження проблем методики розслідування економічних злочинів в кіберпросторі було отримано такі результати:

1) визначено і розкрито елементи криміналістичної характеристики шахрайства в мережі Інтернет та підробки електронних грошей;

2) дані авторські визначення основним термінам, необхідним для розуміння особливостей методики розслідування цього виду злочинів;

3) на основі вивченого матеріалу сформульовані рекомендації по проведенні деяких оперативно-розшукових заходів і слідчих дій, що становлять особливу важливість і складність для розслідування інтернет-шахрайства;

4) розкриті і проаналізовані особливості використання слідчим спеціальних знань на стадії досудового розслідування, а також особливості організації взаємодії з особами, що володіють спеціальними знаннями;

5) розглянуті основні питання призначення судової комп'ютерно-технічної експертизи, а також наведено приблизний список питань, які, в залежності від ситуації, що склалася, доцільно ставити перед експертом;

6) досліджено наукові завдання, які ще потрібно вирішувати у майбутньому, серед яких:

- Організація системи регулювання правовідносин у віртуальних економіках і захисту прав і законних інтересів учасників цих правовідносин.

- Адаптація накопиченого досвіду і знань про розслідування традиційних злочинів під сучасні потреби правоохоронних органів для розслідування злочинів, скоєних в кіберпросорі.

- Розробка нових ефективних методів попередження кіберзлочинності.

- Розробка найбільш ефективних схем взаємодії між правоохоронними органами та потерпілими в цілях досягнення найбільшої довіри при розслідуванні злочинів і ін.

Як можна зауважити, не всі із зазначених завдань вирішуються криміналістикою. Тому потрібне комплексне дослідження механізмів протидії науковцями і практиками в таких сферах, як цивільне право, економіка, кримінальне право, кримінальний процес та нормотворча діяльність.

Крім того, говорячи про криміналістику, слід зазначити, що поставлені в цьому дослідженні питання потребують подальшого вивчення. Оскільки інтернет-злочинність розвивається надзвичайно швидко, актуальною видається рекомендація продовжувати вивчення проблем методики розслідування економічної кіберзлочиності з метою накопичення нових і актуалізації старих знань, отриманих в інших дослідженнях з даної тематики. Проведене наукове дослідження дозволило сформувати нам ряд конкретних висновків.

1. Шахрайство в мережі Інтернет має ряд відмінностей у порівнянні з традиційним шахрайством. Ці відмінності зумовлюють особливості розслідування даного злочину. Зокрема, такі особливості проявляються при здійсненні оперативно-розшукових заходів і слідчих дій.

2. Проведення оперативно-розшукових заходів і слідчих дій при розслідуванні інтернет-шахрайства ускладнюється тим, що частина здобутої при їх проведенні інформації збувається з джерел віртуальної інформації (комп'ютер потерпілого або злочинця, віддалений локальний сервер, мережа Інтернет і т.д.)

3. Застосування спеціальних знань при розслідуванні кіберзлочинів вимагає також від слідчого знання високих інформаційних технологій для визначення необхідної спеціалізації, якою повинен володіти експерт і спеціаліст, а також для найбільш продуктивної взаємодії з зазначеними особами на всіх етапах досудового розслідування інтернет-шахрайства.

Подальший пришвидшений розвиток Інтернет-технологій буде лише каталізатором Інтернет-злочинності, тому правоохоронні органи та суди мають бути до цього готові. Створення підрозділів Кіберполіції є першим кроком на шляху до вирішення означених у нашому дослідженні проблем, та все ж не гарантією повного успіху. Працівники кіберполіції мають мати доступ до найважливіших досягнень науки і техніки, постійно вивчати нові можливості

Інтернет-злочинності і мати можливість діяти на випередження злочинців. Тільки в такому разі можна буде говорити про ефективну протидію економічним злочинам, що вчиняються в кіберпросорі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Анапольська А. І. Розслідування шахрайства і пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність»/ Анапольська А. І. – Х., 2011. – 18 с.
2. Андрушко П. П. Коментар до розділу XVI «Злочини у сфері використання електроннообчислювальних машин (комп'ютерів), системи та комп'ютерних мереж і мереж електорозв'язку» Особливої частини КК України // П. П. Андрушко. Законодавство України. – 2005. – № 3. – С. 65-87.
3. Арешонков В. В. Окремі міжнародно-правові проблеми боротьби з кіберзлочинністю в умовах глобалізації / В. В. Арешонков // Вісн. Луган. держ. ун-ту внутр. справ. Спец. вип. – 2013. – № 5. – С. 173-176.
4. Ахтирська Н. Комп'ютерна злочинність в Україні через призму судової практики / Н. Ахтирська, В. Антощук // Вісн. прокуратури. – 2018. –№ 3. – С.84-95.
5. Баєв О. О. Боротьба з кіберзлочинністю: правовий та виховний аспекти / О. О. Баєв // Спеціальна техніка у правоохоронній діяльності : матеріали V міжнар. наук.-практ. конф. (Київ, 25 листоп. 2011 р.). – К. : Нац. акад. внутр. справ України, 2012. – С. 194-197.
6. Бельський Ю. Щодо визначення поняття кіберзлочину / Ю. Бельський // Юридичний вісник. — 2014. — № 6. — С. 414-418
7. Біленчук П. Д. Кіберзлочинність: загрози, ризики, небезпеки XXI століття // П. Д. Біленчук, В. Г. Хахановський, О. О. Шульга // Спеціальна техніка у правоохоронній діяльності : матеріали IV Міжнар. наук.-практ. конф. (Київ, 26-27 листоп. 2009 р.). – К. : Київ. нац. ун-т внутр. справ, 2009. – С. 124-125.
8. Біленчук П. Д. Комп'ютерна злочинність: поняття, сутність, характеристика / П. Д. Біленчук, О. О. Шульга // Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх

справ: стан, проблеми та 13 шляхи вирішення : матеріали всеукр. наук.-практ. конф. 9 груд. 2011 р. – Донецьк : Донец. юрид. ін-т, 2012. – С. 28-31

9. Біленчук П. Д. Способи вчинення комп'ютерних злочинів у кредитнофінансовій сфері / П. Д. Біленчук, О. О. Шульга // Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення : матеріали всеукр. наук.-практ. конф. 9 груд. 2011 р. – Донецьк : Донец. юрид. ін-т, 2012. – С. 24-28.

10. Білоус В.Т. Координація боротьби з економічною злочинністю: Монографія. - Ірпінь: Академія державної податкової служби України, 2002. - 449 с.

11. Браточкін М. О. Проблемні питання організації розслідування фактів несанкціонованого переказу коштів з рахунків клієнтів банку, які обслуговуються за допомогою систем дистанційного обслуговування / М. О. Браточкін // Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – С. 197-201.

12. Бурда С. Я. Окремі питання кримінальної відповідальності за посягання у сфері інформаційної безпеки / С. Я. Бурда, А. О. Йосипів // Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – С. 108-112.

13. Бутузов В. М. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : Науково-практичний коментар / В. М. Бутузов, С. Л. Остапець, В. П. Шеломенцев; МВС України. Департамент ДСБ з економічною злочинністю. – К., 2005. – 86 с

14. Бутузов В. М. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток : [навч. посіб.] / В. М. Бутузов, В. І. Василинчук, В. П. Шеломенцев; МВС України. Департамент ДСБ з економічною злочинністю. КНУВС. ННІПККМ. – К., 2006. – 139 с.

15. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системноструктурний аналіз) : [моногр.] / Бутузов В. М.; РНБО України. МНДЦ з проблем б-би з орг. злочинністю. – К. : КИТ, 2010. – 405 с.

16. Бутузов В. М. Співвідношення понять «комп'ютерна злочинність» і «злочинність у високих інформаційних технологій» / В. М. Бутузов // Боротьба з 6 організованою злочинністю і корупцією (теорія і практика). – К. : МНДЦ, 2010. – № 23. – С. 302-308.

17. Бутузов В. Н. Противодействие преступности в сфере использования банковских платежных карточек в условиях глобализации / В. Н. Бутузов // Організація і тактика документування підрозділами ДСБЕЗ злочинів у комп'ютерних мережах та мережах електрозв'язку : матеріали всеукр. наук. – практ. конф., 4 груд. 2009 р. – Донецьк : Донец. юрид. ін-т, 2009. – С. 24-28.

18. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : [монографія] / В. Бутузов. – К. : КИТ, 2010. – 148 с.

19. Буяджи С.А. Правове регулювання боротьби із кіберзлочинністю: теоретико-правовий аспект: автореф. дис. ... канд юрид. наук : 12.00.01 / С.А. Буяджи; Класичний приватний університет. Івано-Франківськ, 2018. – 18 с.

20. Взаємодія правоохоронних органів з провайдерами та операторами зв'язку в боротьбі з комп'ютерними злочинами : матеріали регіон. наук.-практ. сем., 12 груд. 2008 р. / Донецький юрид. ін-т. – Донецьк, 2009. – 151 с.

21. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій : [моногр.] / МВС України, Донецький юрид. ін-т / І. Ф. Хараберюш, В. Я. Мацюк, В. А. Некрасов, О. І. Хараберюш. – К. : КНТ, 2007. – 195 с.

22. Вовк В. Я. Кіберзлочинність у банківській сфері : наслідки та шляхи протидії / В. Я. Вовк // Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – С. 187-191.

23. Вознюк А. А. Організовані злочинні об'єднання в мережі Інтернет: кримінально-правовий аспект / А. А. Вознюк // Боротьба з інтернет-

злочинністю : матеріали міжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). – Донецьк : Донец. юрид. ін-т, 2013. – С. 68-70.

24. Воронов І. О. Організація протидії злочинам у сфері використання платіжних карток та інших засобів доступу до банківських рахунків / І. О. Воронов // Південноукраїнський правничий часопис. – 2010. – № 1. – С. 26-29.

25. Воронов І. О. Феномен BOTNET – латентна мобілізація сегментів мережі Інтернет для вчинення злочинів у сфері високих інформаційних технологій / І. О. Воронов // Вісн. Луган. держ. ун-ту внутрішніх справ. – Луганськ, 2010. – № 3. – С. 275-287.

26. Всесвітнє дослідження економічних злочинів та шахрайства 2018 року: результати опитування українських організацій Виведення шахрайства з тінihttps ://www.pwc.com/ua/uk/survey/2018/pwc-gecs-2018-ukr.pdf

27. Голік А.В. Боротьба з кіберзлочинністю : навч. – метод. матеріали з англ. мови (спецкурс) для підготовки фахівців для підрозділів по боротьбі з кіберзлочинністю. – К. : Нац. акад. внутр. справ, 2016. – 32 с.

28. Голубєв В. О. Конвенція щодо боротьби з кіберзлочинністю як елемент правового механізму взаємодії правоохоронних органів з провайдерами та операторами зв’язку в боротьбі з комп’ютерними злочинами / В. О. Голубєв // Взаємодія правоохоронних органів з провайдерами та операторами зв’язку в боротьбі з комп’ютерними злочинами : матеріали регіон. наук.-практ. сем., 12 груд. 2008 р. – Донецьк : Донец. юрид. ін-т, 2009. – С. 43-49.

1. Гринчак І. В. Кіберзлочинність як злочин міжнародного характеру /І. В. Гринчак // Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. - 2015. - № 12. - С. 93-98.

29. Громико І. О. Виявлення несанкціонованого безконтактного підключення до інформаційних мереж / І. О. Громико, С. Ю. Кільмаєв, М. В. Цуранов // Протидія злочинності у сфері інтелектуальної власності та комп’ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення : матеріали всеукр. наук.-практ. конф. 9 груд. 2011 р. – Донецьк : Донец. юрид. ін-т, 2012. – С. 36-39.

30. Грубий М. В. Шляхи вдосконалення міжнародного співробітництва у сфері протидії кіберзлочинності / М. В. Грубий // Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення : матеріали всеукр. наук.-практ. конф. 9 груд. 2011 р. – Донецьк : Донец. юрид. ін-т, 2012. – С. 39-42.

31. Діордіца І. В. Адміністративно-правове регулювання кібербезпеки України : автореф. дис. ... д-ра юрид. наук : 12.00.07 / Діордіца Ігор Володимирович ; Запоріз. нац. ун-т. - Запоріжжя, 2018. - 32 с.

32. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003 р. // Офіційний вісник України. — 2010 р., № 56, / № 31, 2006, ст. 2202 /, — стор. 73, — стаття 1920.

33. Европейская Конвенция по киберпреступлениям от 23 ноября 2001 г. / [Електронний ресурс] – Режим доступу:http://www.eos.ru/eos_delopr/eos_law/detail.php?ID=32003&SECTION_ID=671

34. Енциклопедія сучасної України // http://esu.com.ua/search_articles.php?id=18798

35. Єдиний державний реєстр судових рішень //www.reyestr.court.gov.ua/

36. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2016 року // Відомості Верховної Ради України (ВВР), 2006, № 30, ст.258

37. Закон України про ратифікацію Конвенції про кіберзлочинність : прийн. 7 верес. 2005 р. // Офіційний вісн. України. – 2005. – № 39. – Ст. 2437.

38. Зацеркляний М. М. Загальні питання слідоутворення в інформаційних компонентах комп'ютерних систем / М. М. Зацеркляний, О. В. Струкова // Протидія кіберзлочинності в фінансово-банківській сфері :

матеріали Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – С. 100-103.

39. Збірник методичних рекомендацій з викриття злочинів у сфері економіки (документування та викриття злочинів у сфері інтелектуальної власності та комп'ютерних технологій). Ч. 2. /МВС України, ДСБЕЗ. – К., 2009. – 191 с

40. Зимовець В. В. Кіберзлочинність в Україні: перспективи протидії / В. В. Зимовець, Д. Е. Чувирін // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К. : МНДЦ, 2016. – № 13. – С. 99-113.

41. Карчевський М. В. До питання та визначеності термінології при криміналізації злочинів у сфері використання комп'ютерної техніки та мереж електрозв'язку (Розділ XV1) / М. В. Карчевський // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К. : МНДЦ, 2010. – № 23. – С. 302-308.

42. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : моногр. / Карчевський М. В. – Луганськ : Луган. держ. ун-т внутр. справ, 2012. – 327 с

43. КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ. Інформаційно-аналітичний дайджест. - Київ – 2018. – 74 с.

44. Кісілюк І. І. Міжнародне співробітництво у боротьбі з кіберзлочинністю / І. І. Кісілюк // Модернізація Конституції України та вдосконалення правоохоронної діяльності : матеріали підсумк. наук.-практ. конф. (Київ. 25 квіт. 2014 р.); Нац. акад. внутр. справ, Нац. акад. прав. наук. – К., 2014. – С. 286-289.

45. Книженко О. О. Сучасний стан злочинів у сфері використання елктронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку в Україні / О. О. Книженко // Бюлетень Міністерства юстиції України. – 2014. – № 7. – С. 122-128.

46. Кобзев І. В. Використання вільного програмного забезпечення при підготовці фахівців для боротьби з високотехнологічними злочинами у фінансово-банківській сфері / І. В. Кобзев, К. Е. Петров // Протидія

кіберзлочинності в фінансовобанківській сфері : матеріали Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – С. 76-79.

47. Ковалев Д.И. Криминологическая характеристика личности преступника, совершившего преступление в сфере компьютерной информации. Вестник Академии. 2011. № 3. С. 90-94. URL: https://elibrary.ru/item.asp?id=16556890.

48. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X // Відомості Верховної Ради Української РСР (ВВР) 1984, додаток до № 51, ст.1122.

49. Козак Н. С. Визначення злочинів у сфері оподаткування, що вчиняються з використанням комп'ютерних технологій / Н. С. Козак // Актуальні питання реформування правової системи України. – Луцьк, 2018. – С. 484-485.

50. Козак Н.С. Криміналістичні прийоми, способи і засоби виявлення, розкриття та розслідування комп'ютерних злочинів: автореф. дис. ... канд. юрид. наук : 12.00.09 / Н.С. Козак; Національний університет державної податкової служби України. – Ірпінь, 2011. – 21 с.

51. Коліса Я. Ю. Взаємодія служб у боротьбі з кіберзлочинністю / Я. Ю. Коліса // Криміналістичний вісник. - 2015. - № 1. - С. 99-102

52. Конвенція про кіберзлочинність : підпис. 23 листопада 2001р // Офіційний вісник України. – 2007. – №65. – Ст. 2535.

53. Конституція України від 28 червня 1996 року // Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141

54. Корж В.П. Теоретические основы методики расследования преступлений, совершаемых организованными преступными образованиями в сфере экономической деятельности: монография. Харьков, 2012. 412 с.

55. Користін О. Є. Протидія відмиванню коштів в Україні: правові та організаційні засади правоохоронної діяльності : [навч. посіб.] / О. Є. Користін, С. С. Чернявський. – К. : КНТ, 2009. – 612 с. – Р. 6, § 2, 2.5 : Використання поза банківських електронних платіжних систем при відмиванні коштів. – С. 420-426.

56. Котюк І. І. Комп'ютерна злочинність в банківській індустрії / І. І. Котюк, П. Д. Біленчук // Боротьба зі злочинами у сфері комп'ютерної інформації : проблеми та шляхи їх вирішення : матеріали міжвуз. наук.-практ. конф. 14 груд. 2007 р. – Донецьк : Донец. юрид. ін-т, 2008. – С. 65-69.

57. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. ... канд. юрид. наук : 12.00.08 / М. О. Кравцова ; Харк. нац. ун-т внутр. справ. - Харків, 2016. - 16 с.

58. Кравчук С. Й. Економічна злочинність в Україні / С. Й. Кравчук. − [Електронний ресурс]. − Режим доступу: http://westudents.com.ua/knigi/116-ekonomchna-zlochinnst-v-ukran-kravchuk-sy.html

59. Криміналістична профілактика економічних злочинів: Науково-практичний посібник / Кол. авт.: С.В. Веліканов, А.Ф. Волобуєв, В.А. Журавель та ін. (За ред. д-ра юрид. наук, проф. В.А. Журавля). - Х.: "Харків юридичний", 2006. - 236 с.

60. Кримінальний кодекс України: Закон України від 5 квітня 2001 р. // Відомості Верховної Ради України. – 2001. – № 25-26. – Ст. 131.

61. Кримінально-процесуальний кодекс України від 13 квітня 2012 року //Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88.

62. Кузьменко А. Особливості класифікації комп'ютерних злочинів «комп'ютерної інформації» як об'єкта протиправних посягань / А. Кузьменко // Юрид. журн. – 2010. – № 3. – С. 54-58.

63. Курилін І.Р. Використання спеціальних знань при розслідуванні злочинів, які посягають на права інтелектуальної власності: автореф. дис. ... д-ра юрид. наук : 12.00.09/ І.Р. Курилін; Київський національнй університет внутрішніх справ. – Київ, 2007. – 19 с.

64. Литвинов О.М. Кримінологія: питання та відповіді / Кол. авторів: Авдеев О. О., Васильєв А. А. та ін.; за заг. ред. О. М. Литвинова. – Х.: Золота миля, 2015. – 324 с.

65. Літвінов М. Ю. Світова та українська практика боротьби з кіберзлочиністю / М. Ю. Літвінов // Право і безпека. – 2017. – № 1. – С. 85-89.

66. Мазуренко М. С. Протидія податковим злочинам у сфері інформаційних технологій / М. С. Мазуренко, А. В. Шапка // Боротьба з інтернет-злочинністю : матеріали міжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). – Донецьк : Донец. юрид. ін-т, 2013. – С. 136-139.

67. Манжай О. В. Окремі методи захисту банківських платіжних карт / О. В. Манджай, Ю. Г. Машкаров // Протидія кіберзлочинності в фінансовобанківській сфері : матеріали Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – С. 79-82.

68. Марков В. В. Про механізми скоєння злочинів у кіберпросторі та особливості їх кваліфікації / В. В. Марков // Південноукраїнський правничий часопис. – 2013. – № 1. – С. 112-115.

69. Марков В. В. Статистичне дослідження показників кіберзлочинності: методологічний аспект / В. В. Марков // Право і безпека. – 2013. – № 2. – С. 136-140.

70. Марков В. В. Щодо питання стосовно зарубіжного досвіду протидії кіберзлочинності / В. В. Марков Національний юридичний журнал:теорія і практика. - 2015. - С. 187-191.

71. Матусовский ГА. Экономические преступления: криминалистический анализ. - Х.: Консул, 2009. - 274 с.

72. Міщук Н. Кіберзлочинність як загроза інформаційному суспільству / Н. Мыщук // Вісник Львівського університету. Серія економічна. — 2014. — Випуск 51. — С. 173-179

73. Мороз Н. О. Основные этапы развития международно-правового сотрудничества в борьбе с преступностью в сфере высоких технологий / Н. О. Мороз // Проблемы борьбы с преступностью и подготовки кадров для ОВД Республики Бєларусь : тез. докл. Междунар. науч.-практ.конф. (Минск, 30 июня 2010 г.). – Минск : Акад. МВД, 2010. – С. 49-50.

74. Науково – практичний коментар Кримінального кодексу України за ред. М. І. Мельника, м. І. Хавронюка. – 7 – ме видання, переробл. та допов.- К. : Юридична думка, 2010, - стор. 122

75. Небитов А. А. Шахрайство у сфері електронної комерції / А. А. Небитов, Л. В. Лефтеров // Боротьба з інтернет-злочинністю : матеріали міжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). – Донецьк : Донец. юрид. ін-т, 2013. – С. 52-55.

76. Никифорчук Д. Й. Характеристика кіберзлочинів, що вчиняються з метою отримання незаконних доходів / Д. Й. Никифорчук, Є. В. Лизогубенко // Боротьба з інтернет-злочинністю : матеріали міжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). – Донецьк : Донец. юрид. ін-т, 2013. – С. 43-45.

77. Носов В. В. Система управління реагування на інциденти у фінансово-банківській сфері / В. В. Носов // Протидія кіберзлочинності в фінансовобанківській сфері : матеріали Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – С. 43-47.

78. Олиндер Н. В. Типичные способы совершения преступлений с использованием электронных платежных средств и систем / Н. В. Олиндер // Експерт-криминалист. – 2014. – № 1. – С. 13-16.

79. Омельченко О. С. Проблеми протидії кіберзлочинності в кредитно-банківській сфері / О. С. Омельченко // Протидія кіберзлочинності в фінансовобанківській сфері : матеріали Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – С. 96-100.

80. Орлов Ю.Ю. Реалізація вимог Міжнародної конвенції про кіберзлочинність у законодавстві України / Ю. Ю. Орлов // Наук. вісн. Нац. акад. внутр. справ. – К., 2011. – Вип. 6(79). – С. 3–9.

81. Панов М. І. Злочини у сфері обслуговування електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку / Панов М. І. Вибрані наукові праці з проблем правознавства. – К. : Ін Юре, 2010. – С. 758-775.

82. ПетровС. А. Особенности квалификации хищений, совершенных с использованием компьютерной техники / С. А. Петров // Рос. следователь. – 2017. – № 15. – С. 22-25

83. Політова А. С. Міжнародне співробітництво у боротьбі з кіберзлочинністю / А. С. Політова // Боротьба з інтернет-злочинністю :

матеріали міжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). – Донецьк : Донец. юрид. ін-т, 2013. – С. 214-216.

84. Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС 6 наказ МВС України від 30 жовт. 2012 р. № 988 Електронний ресурс. – Режим доступу : http://document.ua/pro-organizaciyu-dijalnostiupravlinnija -borotbi-z-kiberzjoch-130740.html

85. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування : Аналітична записка [Електронний ресурс]. — Режим доступу : http:// www.niss.gov.ua/articles/454

86. Протидія економічній злочинності / П.І. Орлов, А.Ф. Волобуєв, І.М. Осика та ін. - Харків: Нац. ун-т внутр. справ, 2014. - 568 с.

87. Протидія кіберзлочинності в Україні: правові та організаційні засади : [навч. посіб.] / О. Є Користін, В. М. Бутузов, О. А. Безуглий та ін. – К. : «Скіф», 2012. – 728.

88. Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – 285 с.

89. Пфо, О. М. Основні поняття і класифікація кіберзлочинності / О. М. Пфо // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23-25 листоп. 2016 р. — Кропивницький : КНТУ, 2016. — С. 33-34.

90. Пчеліна О. В. Механізм вчинення економічних злочинів / О. В. Пчеліна // Право і Безпека. − 2009. − № 4.− С. 118−122.

91. Рогозін С. М. Інфомаційно-правові засади протидії економічній злочинності / С. М. Рогозін // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К. : МНДЦ, 2012. – № 1. – С. 289-295.

92. Розкриття та розслідування кіберзлочинів : зб. метод. реком. Ч.1. – К. : НАВС, 2010. – 257 с.

93. Савченко А. В. Особливості кримінально-правової кваліфікації несанкціонованого втручання в роботу вбудованих комп'ютерних систем / А. В. Савченко, М. В. Карчевський // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К. : МНДЦ, 2013. – № 2. – С. 254-260.

94. Самойленко О. А. Класифікація типових слідів вчинення викрадення майна з використанням комп'ютерних технологій / О. А. Самойленко // Вісн Луган. акад. внутр. справ МВС. Спец. вип. – 2005. – Ч. 2. – С. 25-29.

95. Скулиш Є. Д. Міжнародно-правове співробітництво у сфері подолання кіберзлочинності / Є. Д. Скулиш // Інформація і право. - 2018. - № 1. - С. 93-100.

96. Словник термінів з кібербезпеки / РНБО України, Нац. акад. СБУ; за заг. ред. О. В. Копана, Є. Д. Скулиша. – К., 2012. – 213с.

97. Струкова В. Є. Доступність кіберпростору і кіберзлочинність / В. Є. Струкова // Боротьба з інтернет-злочинністю : матеріали міжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). – Донецьк : Донец. юрид. ін-т, 2013. – С. 236-238.

98. Стюарт Мак-Клар. Секреты хакеров. Безопасность сетей / С. Мак-Клар, Д. Скембрей, Курц Д. [Электронный ресурс]. – Режим доступа : http:www://crimeresearch.ru

99. Судова практика розгляду про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку // Вісник Верховного Суду України. – 2017. – № 2. – С. 29-34.

100. Тарасюк А. В. Використання спеціальних знань спеціаліста та експерта в протидії кіберзлочинності / А. В. Тарасюк, К. В. Басін // Спеціальна техніка у правоохоронній діяльності : матеріали V міжнар. наук.-практ. конф. (Київ, 25 листоп. 2011 р.). – К. : Нац. акад. внутр. справ України, 2012. – С. 184-186.

101. Тихомиров О.О. Кіберзлочин: теоретико-правові проблеми / О.О. Тихомиров // Зб. матеріалів наук.-практ. конф. "Інформаційна безпека:

виклики і загрози сучасності"; 5 квітня 2013 р. — К. : Наук.-вид. центр НА СБ України. — 2013. — С. 179-182

102. Фактори детермінації кіберзлочинності в сучасній кримінологічній теорії. Кварцова М. О. Юридичний науковий електронний журнал. № 5/2014 http://www.lsej.org.ua/5_2014/31.pdf

103. Фріс П. Л. Кримінально-правова політика у сфері протидії кіберзлочинності в Україні: ефективність та перспективи розвитку / П. Л. Фріс, Н. А. Савінова // Боротьба з інтернет-злочинністю : матеріали міжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). – Донецьк : Донец. юрид. ін-т, 2013. – С. 39-43.

104. Харко Д. М. Кримінологічні проблеми щодо визначення поняття та ознак сучасної економічної злочинності як фактора тінізації економіки України / Д. М. Харко. − [Електронний ресурс]. − Режим доступу: http://www.apdp.in.ua/v55/119.pdf

105. Хахановський В. Г. Особливості криміналістичної характеристики кіберзлочинів / В. Г. Хахановський // Юрид. часопис Нац. акад. внутр. справ. – К., 2018. –№1(1). – С.89-93.

106. Хахановський В. Г. Проблеми боротьби з організованою кіберзлочинністю в економічній сфрі / В. Г. Хахановський // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К. : МНДЦ 2013. – № 2. – С. 79-84.

107. Хахановський В.Г. Теорія і практика криміналістичної інформатики : автореф. дис. ... докт. юрид. наук : 12.00.09 / В.Г. Хахановський; Національна академія внутрішніх справ. – Київ, 2011. – 30 с.

108. Хилюта В. Компьютерные хищения / В. Хилюта // Законность. – 2009. – № 1. – С. 36-38.

109. Чернєй В. В. Зарубіжний досвід запобігання фінансовому шахрайству / В. В. Чернєй // Кримінологічна теорія і практика: досвід, проблеми сьогодення та шляхи їх вирішення : тези доп. наук.-теорет. конф. (Київ, 20 берез. 2014 р.). – К. : Нац. акад. внутр. справ, 2014. – С. 9–12.

110. ЧернявськийС. С. Фінансове шахрайство : методологічні засади розслідування : моногр. / С. С. Чернявський. – К. : «Хай-Тек-Прес», 2010. – Р. 3.3.6 : Основи методики розслідування шахрайства у сфері використання комп'ютерних мереж. – С. 384-393.

111. Шабашкевич С. В. Мошенничество с ичпользованием дистанционного банковского обслуживания (ДБО), способы противодействия / С. В. Шабашкевич // 40 Боротьба з інтернет-злочинністю : матеріали міжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). – Донецьк : Донец. юрид. ін-т, 2013. – С. 60-62.

112. Шавиркін Б. В. Деякі особливості розслідування кіберзлочинів / Б. В. Шавиркін // Боротьба з інтернет-злочинністю : матеріали міжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). – Донецьк : Донец. юрид. ін-т, 2013. – С. 124-128.

113. Шапочка С. В. Боротьба з шахрайством, що вчиняється в мережі Інтернет / С. В. Шапочка // Боротьба з інтернет-злочинністю : матеріали міжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). – Донецьк : Донец. юрид. ін-т, 2013. – С. 99-100.

114. Шапочка С. В. До питання запобігання окремим видам шахрайства, яке вчиняється з використанням можливостей мережі Інтернет / С. В. Шапочка // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К. : МНДЦ 2014. – № 1. – С. 145-150.

115. Шеломенцев В. П. Організована кіберзлочинність: до визначення поняття / П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К. : МНДЦ, 2017. – № 21. – С. 307-314.