МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ БІЗНЕСУ І ПРАВА
КАФЕДРА НАЦІОНАЛЬНОГО, МІЖНАРОДНОГО ПРАВА ТА ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ПЕРЕШКОДЖАННЯ РОБОТІ ЕОМ АВТОМАТИЗОВАНИХ СИСТЕМ, КОМП'ЮТЕРНИХ МЕРЕЖ ЧИ МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ ШЛЯХОМ МАСОВОГО РОЗПОВСЮДЖЕННЯ ПОВІДОМЛЕНЬ ЕЛЕКТРОЗВ'ЯЗКУ

Кваліфікаційна робота (проєкт)
на здобуття ступеня вищої освіти «магістр»

Виконала: студентка 2 курсу 10-281 МЗ групи
Спеціальності 262 Правоохоронна діяльність
Освітньо-професійної програми
«Правоохоронна діяльність»
Шкловець Юлія Ігорівна

Керівник: к.ю.н., доцент **Проценко М.В.**
Рецензент:
адвокат Адвокатського бюро: «Юрія Карпухіна»
Карпухін Ю.Ю.

Херсон – 2021

ЗМІСТ

ВСТУП

Актуальність теми. Істотною перешкодою для розбудови в Україні демократичної, правової держави є високий рівень злочинності в нашій державі. Зокрема, мова йде про кіберзлочинність. Застосування кіберзлочинцями новітніх технологій та обладнання, об’єднання у стійкі, добре організовані групи – все це робить боротьбу з ними складним завданням.

Питання, пов’язані з боротьбою з кіберзлочинністю, раніше були предметом досліджень таких вчених, як П.П. Андрушко, Ю.М. Батурін, П.Д. Біленчук, М.С. Вертузаєв, В. Д. Гавловський, О. І. Гарасимів, В.Г. Гончаренко, М.В. Гуцалюк, . М. Дуфенюк, В. А. Журавель, О. В. Захарова, М.І. Панов, А.М. Ришелюк, Б.В. Романюк,и В. П. Сабадаш, А. В. Самодін, В. Ю. Шепітько, Ю. М. Чорноус. Однак, незважаючи на значний внесок досліджень вказаних вчених в розвиток правової науки, низка проблемних питань досліджена лише фрагментарно. До них відносяться, зокрема, проблемні питання, пов’язані з особливостями розслідування перешкоджання роботі ЕОМ автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку. Удається за необхідне провести дослідження зазначених питань.

Мета і задачі дослідження. Метою дослідження є дослідження особливостей розслідування перешкоджання роботі ЕОМ автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

Для досягнення даної мети були сформовані такі **завдання:**

- дослідити суспільну небезпечність кіберзлочинів;
- проаналізувати криміналістичні відомості про кіберзлочинців;

– дослідити особливості розслідування перешкоджання роботі мереж електрозв'язку, комп'ютерних мереж, роботі комп’ютерів та автоматизованих систем, що вчиняються з мотивів помсти, ненависті, інших неприязних стосунків;

– проаналізувати особливості розслідування перешкоджання роботі мереж електрозв'язку, комп'ютерних мереж, роботі комп’ютерів та автоматизованих систем, що вчиняються з корисливих мотивів.

Об’єктом дослідження є суспільні відносини, пов’язані із особливостями розслідування перешкоджання роботі ЕОМ автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

Предметом дослідження є результати наукових досліджень, правові норми, за допомогою яких визначаються особливості розслідування перешкоджання роботі ЕОМ автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

Методи дослідження обрані, виходячи із мети і завдань роботи, а також із врахуванням об’єкта і предмета дослідження. В основу дослідження покладено метод ідеалістичної діалектики як фундаментальний (філософський) метод наукового пізнання.

При проведенні дослідження використовувались загально наукові методи: формально-юридичний, статистичний, порівняльно-правовий, системно-структурний, порівняльний, описовий, експериментальний, ряд логічних методів (аналізу, синтезу, індукції, дедукції, аналогії, версії та ін.).

Наукова новизна одержаних результатів полягає в тому, що представлена робота робить спробу комплексного дослідження особливостей розслідування перешкоджання роботі ЕОМ

автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

Практичне значення роботи полягає у виявленні основних проблемних питань щодо особливостей розслідування перешкоджання роботі ЕОМ автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку. У роботі сформульовані висновки, пропозиції та рекомендації можуть бути використані в подальшому дослідженні даної теми, а окремі положення та висновки роботи – в процесі підготовки і проведення практичних занять з курсу «Криміналістика», «Кримінальний процес».

Апробація результатів дослідження. Основні положення дослідження були представленні на ІІ-му дискусійному форумі «Сучасні проблеми державотворення та право» організованому ГО УКРАЇНСЬКО-СЛОВАЦЬКИЙ ЦЕНТР ПАРТНЕРСТВА (29 листопада 2021 р., м. Херсон).

Структура роботи обумовлена метою та завданнями дослідження і складається із вступу, двох розділів, які поділяються на чотири підрозділи, висновків, списку використаних джерел. використаних джерел налічує 40 найменувань.

РОЗДІЛ 1
ЗАГАЛЬНІ ВІДОМОСТІ ЩОДО РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

1.1. Суспільна небезпечність кіберзлочинів

Слушним, на нашу думку, удається розгляд проблемних питань щодо суспільної небезпечності кіберзлочинів.

«Сучасна школа критичної геополітики та частина американських фахівців дедалі частіше вказують на те, що для кіберпростору мають застосовуватися суттєво модернізовані, проте за суттю ті самі підходи, які були сформульовані класиками геополітики, передусім американцями Х. Маккіндером (*Halford John Mackinder*) і Н. Спайкменом (*Nicholas John Spykman*). Наприклад, дослідники Ф. Крамер (*Franklin D. Kramer*), С. Старр (*Stuart H. Starr*) та Л. Вентц (*Larry Wentz*) зазначають із цього приводу: «так само, як Макіндер та Спайкмен визначили для «земельної могутності» (*land power*), ті, хто розвиватиме теорію кібермогутності, мають визначити ключові ресурси та основні точки для кіберпростору» [12].

Суспільна небезпечність кіберзлочинів залежить, на думку автора, від наступних факторів:

– вид і розмір збитку. Очевидно, що більш суспільно небезпечними є ті з комп'ютерних злочинів, які мають на увазі насильство (в порівнянні з тими, які лише завдають матеріальної шкоди). Також більш пріоритетними є злочини, які посягають на права неповнолітніх та інших менш захищених суб'єктів;

– поширеність. Як відомо, розкриття злочину і покарання злочинця також в деякій мірі впливають на потенційних правопорушників. Тому розкривати часто зустрічаються типи злочинів при інших рівних важливіше, ніж рідкісні типи злочинів;

– кількість і кваліфікація персоналу. Залежно від того, скільки є співробітників і наскільки вони кваліфіковані, варто братися за ті чи інші комп'ютерні злочини. Занадто складні починати розслідувати марно;

– юрисдикція. Кращими є злочини, які не потребують задіяти іноземні правоохоронні органи. Найбільш швидкий результат виходить при розслідуванні злочинів, локалізованих в межах одного міста;

– політика. Залежно від поточних політичних установок, можуть бути визнані більш пріоритетними деякі види комп'ютерних злочинів. Чи не тому, що вони більш суспільно небезпечні, але тому, що їх розкриття спричинить більший піар-ефект або більше схвалення начальства.

«На тлі позитивних тенденцій розвитку інноваційних технологій у сучасному суспільстві виникло абсолютно нове негативне явище, що отримало назву «комп’ютерна злочинність». Комп’ютерні злочини вирізняються високою латентністю, оскільки існує певна складність для їх виявлення і розкриття. Докази за ними можуть бути знищені за лічені секунди, а ідентифікувати комп’ютер, за допомогою якого здійснено неправомірний доступ, дуже складно. До зброї кіберзлочинця можна додати: комп’ютерні віруси, програмні закладки, різноманітні види віддалених атак, що дозволяють отримати несанкціонований доступ до комп’ютерної системи. Тут відсутні які-небудь форми контролю, що відкриває необмежені можливості для доступу до будь-якої інформації, щораз ширше використовувані в злочинній діяльності, яка набуває транснаціонального, організованого і групового характеру» [32].

1.2. Криміналістичні відомості про кіберзлочинців

Розглянемо характерні особливості кіберзлочинців.

1. «Хакер». Основною мотивацією цього типу порушників є: дослідницький інтерес, цікавість, прагнення довести свої можливості,

честолюбство. Засоби захисту комп'ютерної інформації, її недоступність вони сприймають як виклик своїм здібностям. Характерними є хороші знання в області IT і програмування. Однак зустрічаються хакери, серед яких середній рівень знань виявився невисокий.

Для окремої категорії хакерів, так званих «script kiddies». Характерно те, що керуються тими самими мотивами, але не в змозі придумати своє і тому просто бездумно використовують готові інструменти, зроблені іншими.

Першою рисою особистістю «хакера» є ескапізм – втеча від дійсності, прагнення піти від реальності, від загальноприйнятих норм суспільного життя в світ ілюзій, або псевдодіяльності. Комп'ютерний світ, особливо разом з Інтернетом, є прекрасним альтернативним світом, в якому можливо знайти цікаве заняття, захист від небажаних соціальних контактів, реалізувати креативний потенціал і навіть заробити грошей. З іншого боку, людина, яка чимось сильно захоплена в реальному світі, навряд чи зможе знайти достатню кількість часу і сил, щоб стати хорошим фахівцем в специфічних областях IT.

Ескапізм є фактором для виникнення комп'ютерної або мережевий залежності. Така залежність (в слабкій або сильній формі) є другою рисою особистості ймовірного злочинця. Комп'ютерна залежність (адикція) може початися з звичайного захоплення, яке аддикцією не є. Залежність у важчій формі ближче до психічної девіації, а у важкій формі деякі вважають таку аддикцію хворобою (причому епідемічного характеру), яку слід лікувати.

Комп'ютерна, або мережева аддикція характеризується нездатністю людини відволіктися від роботи в Мережі, дратівливістю при вимушених відволікання, готовністю знехтувати цінностями (матеріальними і соціальними) реального світу заради світу віртуального, зневагою своїм здоров'ям. Дослідження показують, що особи, які страждають мережевий залежністю, в той же час

відрізняються високим рівнем абстрактного мислення, індивідуалізмом, Інтровертний, емоційною чутливістю і деякою мірою нонконформізму.

Ці риси призводять до того, що «хакер» має вузьке коло спілкування і надає перевагу мережеві контакти всім іншим. Шукати його спільників і джерела інформації про нього слід перш за все серед його віртуальних знайомих. Контакти та соціальні зв'язки в реальному світі «хакер» суб'єктивно оцінює як менш комфортні і не схильний довіряти своїм офлайнових знайомим.

Інший наслідок ескапізму – нехтування хакером тим, що існує лише в реальному світі і ніяк не відображено в Мережі. Наприклад, такий фахівець може досить чисто знищити сліди, що залишаються на комп'ютерних носіях (всілякі комп'ютерні логи, тимчасові файли, інформацію в своп тощо), але йому навіть не прийде в голову думка про логи телефонних з'єднань, за допомогою яких він виходив в Мережу.

Іншою рисою особистості хакерів є некримінальна в загальному спрямованість думок «хакера». Дослідницький інтерес і честолюбство не часто поєднуються з антигромадськими установками, побоюванням правоохоронних органів. Це, як правило, призводить в приділення недостатньої уваги приховуванню слідів, невжиття заходів конспірації. Часто у нього навіть відсутнє саме усвідомлення того факту, що ним вчиняється кримінальне правопорушення.

Слід згадати, що ескапізмом і низькою соціалізованістю страждає більшість IT-фахівців. Власне, деякий відрив від реального життя – це побічний ефект великого досвіду в комп'ютерній сфері. Тому пошук по зазначеним критеріям дасть не тільки можливого злочинця, але і цілком законослухняних IT-фахівців.

«Хакери – це узагальнена назва людей, які здійснюють несанкціоноване проникнення в комп’ютерні системи. Дослівно хакер – комп’ютерний хуліган, який отримує задоволення від того, що проник до чужого комп’ютера для забави чи розваг, як правило, не

переслідуючи матеріальних цілей та не завдаючи шкоди. Основна мета хакерів – насолодитися перемогою над комп’ютерним захистом, розширити відкритий кіберпростір, довести свою перевагу і могутність в електронному світі. Свою діяльність вони здійснюють шляхом втручання в комп’ютерні системи, маючи на меті різноманітні цілі. Через складність системи захисту вона для хакера є привабливою. Зазвичай вони мають відмінні знання про деякі системи захисту інформації та пропагують відкритість електронного простору і програмного забезпечення» [32].

2. «Інсайдер». Більш поширеним типом комп'ютерного зловмисника є людина, не занадто добре володіє знаннями в області IT, зате володіє доступом в інформаційну систему (ІС) в силу службового становища. Більша частина «зламів» комп'ютерних систем відбувається зсередини.

При розслідуванні незаконного втручання «інсайдер» – перша версія, яку слід розглядати. Навіть якщо неправомірний доступ був явно зовні, швидше за все, він став можливим через змову з місцевим співробітником. Якщо для «зовнішнього» хакера виявити вразливість в інформаційній системі являє собою завдання, то для співробітника підприємства майже всі уразливості видно з самого початку. І якщо інформаційна система (ІС) має відношення до грошей, цінностей або платних послуг, то співробітник постійно перебуває під спокусою. Однак керівники і навіть співробітники служби безпеки, чиїм піклуванням довірена така ІС, часто страждають дивним дефектом зору: вони побоюються і приділяють увагу захисту від зовнішніх зловмисників і в той самий час сліпо довіряють власним співробітникам, забуваючи, що різниця між першими і другими – тільки в їх можливостях. У співробітників можливостей нашкодити незрівнянно більше. Отже, типовий «інсайдер» вчиняє комп'ютерне злочин (особисто або в формі підбурювання, спільно з «зовнішнім»

співучасником) з використанням відомостей, отриманих в силу службового положення. Такі відомості – паролі, знання про конфігурацію ІС, знання про її слабкі місця, про прийнятих процедурах. У ряді випадків цими відомостями він володіє «офіційно», тобто вони йому необхідні для виконання роботи. Але частіше буває, що реальний доступ співробітників до конфіденційної інформації значно ширше, ніж формальний або чим необхідний. Тобто «інсайдер» знає про ІС більше, ніж йому належить знати.

Наприклад, в одній компанії-операторі зв'язку мав місце інцидент з неправомірним доступом до бази даних. Були змінені дані про обсяг наданих клієнту послуг, від чого компанія зазнала суттєвих збитки. Як виявилося, злочинцем був один із співробітників, вступив в змову з клієнтом, з якого і «списав» частину заборгованості за послуги. Він мав свій власний логін в зазначену базу даних, але вважав за краще скористатися логіном свого начальника. Це не склало особливих труднощів, оскільки той тримав пароль на аркуші паперу, приклеєному до монітора. Звалити провину на колег – характерна поведінка для «інсайдера». «Інсайдер» може вважати себе скривдженим, обділеним керівництвом.

3. «Білий комірець». Цей тип злочинця являє собою давно і добре відомого казнокрада, який змінив «інструменти» своєї діяльності на комп'ютер. Вкрасти у держави або у приватній компанії можна багатьма способів. Крім банального розкрадання тут можливі хабар, комерційний підкуп, незаконне використання інформації, що становить комерційну таємницю, різні види шахрайства тощо. На відміну від «інсайдера», цей тип зловмисника має мінімальну кваліфікацію в сфері ІТ і комп'ютер як знаряддя вчинення злочину не використовує. Комп'ютер тут виступає лише як носій слідів, доказів вчинення злочину.

За своїми мотивами «білі комірці», у свою чергу, поділяються на наступні групи:

– особи, які зловживають своїм службовим становищем з почуття образи на компанію або начальство. Їх слід шукати серед співробітників, які довго пропрацюю на посаді. До того ж, для виникнення мотиву помсти зовсім не обов'язкова наявність дійсної образи з боку роботодавця. В значній частині випадків образи ці виявляються вигаданими. Такий «ображений» співробітник-зловмисник найчастіше краде, щоб «компенсувати» нібито недоотриману від роботодавця зарплатню. Але бувають і безкорисливі месники, які не набувають вигоди від своїх незаконних дій або з етичних міркувань (рідше), або для зниження ймовірності розкриття злочину (частіше).

– безпринципні розкрадачі, які не мають моральних бар'єрів і крадуть тільки тому, що випала така можливість. Для подібних «білих комірців» характерний недовгий термін служби на посаді до початку зловживань. Досить часто за таким є кримінальне минуле.

3. «Вимушені» розкрадачі, що потрапили в скрутне матеріальне становище, в матеріальну чи іншу залежність від особи, яка потребує вчинити викрадання або шахрайство. Як правило, подібні проблеми важко приховати від оточуючих – великий програш, наркоманія, сімейна криза, невдачі в бізнесі. Ця група розкрадачів менш обережна, вони не можуть довго готувати свої злочини, як це роблять перші і другі.

«Е-бізнесмен». Цей тип кіберзлочинців не є кваліфікованим IT-спеціалістом і не має службового становища, яким можна зловжити. З самого початку вони планують саме створення фіктивного підприємства, створеного саме для вчинення злочинів, відмінно усвідомлюючи його протизаконність. Рішення вчинити правопорушення саме в комп'ютерному (мережевому) середовищі, а не в офлайні вони приймають не через наявність особливих знань в цій області і не через внутрішню тягу до комп'ютерів, а виключно на основі раціонального аналізу. Вони порахували, що так їм буде «вигідніше».

«Вигода» комп'ютерного злочину зазвичай пов'язана з його технічної або організаційної складністю. На прості прийоми попадається мало жертв, від простих засобів нападу більшість інформаційних систем давно захищені. Успішні комп'ютерні злочини відрізняються технічною складністю, участю кількох спільників з «поділом праці», багатоходові.

Тому рисою особистості «е-бізнесмена» є наявність організаторських здібностей і підприємницької ініціативи.

Що ж стосується його незаконослухняним, асоціальності, нонконформізму, то автор вважає ці характеристики не обов'язковими. На етапі початкового накопичення капіталу, в умовах так званої «перехідної економіки» багато видів бізнесу передбачають ті чи інші порушення законодавства і асоціальну спрямованість.

Вказаному типу злочинців відповідає більшість кардерів, спамерів і фішерів.

«Антисоціальний тип» (найменування умовне). Також відзначалися інтернет-шахраї, які керувалися не тільки отриманням прибутку. Більш того, їх злочинний дохід часто бував менше, ніж середня зарплата фахівця тієї ж кваліфікації. Мотивом для скоєння шахрайства була антисоціальна психопатія (соціопатія) таких осіб і їх патологічна тяга до ведення подібних «ігор». Социопатія визнана окремим видом психічного розладу і зареєстрована під назвою «antisocial personality disorder» або «dissocial personality disorder» в класифікаторі хвороб ВООЗ). Зазвичай такі типи діють імпульсивно і не схильні до планування, особливо довгострокового. Подібний розлад взагалі часто призводить до скоєння злочину, не тільки комп'ютерного, причому шахрайства частіше, ніж насильства. Інтернет-шахрайство не вимагає особливих технічних знань, цілком достатніх вмінь користуватися готовими програмними інструментами.

Розгляд проблемних питань, пов’язаних з загальними відомостями щодо розслідування кіберзлочинів, дає можливість зробити наступні висновки:

1. Основною мотивацією хакерів є: дослідницький інтерес, цікавість, прагнення довести свої можливості, честолюбство. Засоби захисту комп'ютерної інформації, її недоступність вони сприймають як виклик своїм здібностям. Характерними є хороші знання в області IT і програмування. Однак зустрічаються хакери, серед яких середній рівень знань виявився невисокий.

2. Для окремої категорії хакерів, так званих «script kiddies». Характерно те, що керуються тими самими мотивами, але не в змозі придумати своє і тому просто бездумно використовують готові інструменти, зроблені іншими.

3. Більш поширеним типом комп'ютерного зловмисника є «інсайдер» – людина, не занадто добре володіє знаннями в області IT, зате володіє доступом в інформаційну систему (ІС) в силу службового становища. Більша частина «зламів» комп'ютерних систем відбувається зсередини.

4. При розслідуванні незаконного втручання «інсайдер» – перша версія, яку слід розглядати. Навіть якщо неправомірний доступ був явно зовні, швидше за все, він став можливим через змову з місцевим співробітником. Якщо для «зовнішнього» хакера виявити вразливість в інформаційній системі являє собою завдання, то для співробітника підприємства майже всі уразливості видно з самого початку.

5. «Білий комірець» являє собою давно і добре відомого казнокрада, який змінив «інструменти» своєї діяльності на комп'ютер. Вкрасти у держави або у приватній компанії можна багатьма способів. Крім банального розкрадання тут можливі хабар, комерційний підкуп,

незаконне використання інформації, що становить комерційну таємницю, різні види шахрайства тощо.

6. На відміну від «інсайдера», «білий комірець» має мінімальну кваліфікацію в сфері IT і комп'ютер як знаряддя вчинення злочину не використовує. Комп'ютер тут виступає лише як носій слідів, доказів вчинення злочину.

7. «Е-бізнесмен» як тип кіберзлочинців не є кваліфікованим IT-спеціалістом і не має службового становища, яким можна зловжити. З самого початку вони планують саме створення фіктивного підприємства, створеного саме для вчинення злочинів, відмінно усвідомлюючи його протизаконність.

8. Рішення вчинити правопорушення саме в комп'ютерному (мережевому) середовищі, а не в офлайні «е-бізнесмени» приймають не через наявність особливих знань в цій області і не через внутрішню тягу до комп'ютерів, а виключно на основі раціонального аналізу. Вони порахували, що так їм буде «вигідніше».

9. «Антисоціальні типи» як тип кіберзлочинця відзначаються як інтернет-шахраї, які керувалися не тільки отриманням прибутку. Більш того, їх злочинний дохід часто бував менше, ніж середня зарплата фахівця тієї ж кваліфікації. Мотивом для скоєння шахрайства була антисоціальна психопатія (соціопатія) таких осіб і їх патологічна тяга до ведення подібних «ігор».

10. Суспільна небезпечність кіберзлочинів залежить, на думку автора, від наступних факторів:

– вид і розмір збитку. Очевидно, що більш суспільно небезпечними є ті з комп'ютерних злочинів, які мають на увазі насильство (в порівнянні з тими, які лише завдають матеріальної шкоди). Також більш

пріоритетними є злочини, які посягають на права неповнолітніх та інших менш захищених суб'єктів;

– поширеність. Як відомо, розкриття злочину і покарання злочинця також в деякій мірі впливають на потенційних правопорушників. Тому розкривати часто зустрічаються типи злочинів при інших рівних важливіше, ніж рідкісні типи злочинів;

– кількість і кваліфікація персоналу. Залежно від того, скільки є співробітників і наскільки вони кваліфіковані, варто братися за ті чи інші комп'ютерні злочини. Занадто складні починати розслідувати марно;

– юрисдикція. Кращими є злочини, які не потребують задіяти іноземні правоохоронні органи. Найбільш швидкий результат виходить при розслідуванні злочинів, локалізованих в межах одного міста;

– політика.

11. Залежно від поточних політичних установок, можуть бути визнані більш пріоритетними деякі види комп'ютерних злочинів. Чи не тому, що вони більш суспільно небезпечні, але тому, що їх розкриття спричинить більший піар-ефект або більше схвалення начальства.

РОЗДІЛ 2
ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ОКРЕМИХ ВИДІВ ПЕРЕШКОДЖАННЯ РОБОТІ МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ, КОМП'ЮТЕРНИХ МЕРЕЖ, РОБОТІ КОМП'ЮТЕРІВ ТА АВТОМАТИЗОВАНИХ СИСТЕМ

2.1. Особливості розслідування перешкоджання роботі мереж електрозв'язку, комп'ютерних мереж, роботі комп'ютерів та автоматизованих систем, що вчиняються з мотивів помсти, ненависті, інших неприязних стосунків

Розглянемо криміналістичні особливості наклепу, образ та екстремістські дії в глобальній комп'ютерній мережі Інтернет.

Спосіб вчинення вказаного злочину полягає, як правило, в розміщенні на загальнодоступному, як правило, популярному ресурсі в Інтернеті образливих, наклепницьких або екстремістських матеріалів.

Ресурси можуть бути наступними: веб-форуми і дошки оголошень, веб-сторінки, повідомлення в телеконференціях (newsgroups), масова розсилка (спам) електронною поштою, СМС-повідомленнями та іншими системами обміну повідомленнями. Інші засоби вживаються нечасто.

У деяких випадках зловмисник обмежується одним-двома ресурсами. Швидше за все, це непрофесіонал, який не може або не хоче оцінити охоплену аудиторію. Мало який ресурс охоплює відразу багато користувачів. В інших випадках інформація розміщується на багатьох ресурсах одночасно, і її розміщення періодично повторюється, як того велить теорія реклами.

Одноразове розміщення інформації зловмисник може здійснити власними силами. Для масового розміщення йому доведеться або

залучити професіоналів-спамерів, або знайти, підготувати і задіяти відповідне програмне засіб для масової розсилки або спам-постинга.

Предметом посягання є честь, гідність особи, ділова репутація, національні та релігійні почуття. В деяких випадках метою такої кампанії може бути провокування неправдивого обвинувачення іншої особи в наклепі, образи, екстремізмі; але таке зустрічається не часто.

Розглянемо особливості кіберзлочинців, які найчастіше вчиняють злочини даного виду.

У злочинів переліченої групи загальний не тільки спосіб, але і мотиви. Приниження честі та гідності фізичної особи, нанесення шкоди діловій репутації юридичної особи, образу національних і релігійних почуттів груп людей – все це, як правило, робиться не з корисливих, а з особистих мотивів. Справа в тому, що сама така ідея – образити, обмовити, зганьбити, поглумитися над національністю в Мережі – може прийти в голову лише зопалу, людині, яка не звикла будувати тверезий розрахунок.

Зрозуміло, можливі випадки, коли наклеп в Інтернеті – це частина більшої піар-кампанії, що проводиться з певними корисливими цілями. Але такі випадки рідкісні.

Коли є вибір, яку версію віддати перевагу, «особисту», «ділову» або «політичну», краще починати з особистої. Досвід автора говорить, що більшість правопорушень в Інтернеті (не тільки образи, але і DoS-атаки) зараз диктуються особистими мотивами. Корисливі міркування зустрічаються рідше. Ділових людей в Мережі поки мало і ділових інтересів – теж. Зате особисті образи і амбіції ллються через край.

Зрозуміло з цього, що зловмисника треба починати шукати серед особистих недоброзичливців потерпілого.

Кваліфікація типового злочинця для обговорюваного виду правопорушень знаходиться в чітко окреслених рамках.

З одного боку, він досить щільно спілкується в Інтернеті, щоб надавати значення його впливу на інших людей. Людина, знайомий з глобальною комп'ютерною мережею лише поверхово, навряд чи надають великого значення тому, що написано на якомусь там веб-сайті. Його коло спілкування і його референтна группа1 знаходяться поза Мережею. Його суб'єктивна оцінка значущості і достовірності інформації з Мережі – низька. До того ж він розуміє, що йому буде складно здійснити зазначені дії в малознайомій середовищі.

З іншого боку, рівень знань про мережеві технології такого зловмисника не може бути високим, оскільки тоді він усвідомлював би, як багато слідів залишає кожну дію і скільки є способів його виявити. Новачки, потрапивши в Інтернет, як правило, побоюються «великого брата» і побоюються за свою приватність. Користувач середньої кваліфікації впевнений, що в Інтернеті можна легко досягти анонімності, якщо тільки прийняти відповідні заходи. А мережевий професіонал знає, що ніякі заходи анонімності не забезпечують.

Тобто ймовірний злочинець досить багато часу проводить в Інтернеті, але знає про нього не дуже багато. Таке рушійний почуття, як образа, зазвичай розвивається поступово. І якщо вже підозрюваному прийшло в голову розмістити наклеп або образу саме в Інтернеті, логічно припустити, що там же, в Інтернеті, його світле почуття образи росло і розвивалося. Має сенс розшукати на веб-сайтах і в листуванні попередні суперечки, претензії, негативну інформацію, у відповідь на яку підозрюваний затіяв свою кампанію.

Розглянемо характерні особливості обстановки вчинення злочинів даного виду.

Кілька слів про екстремізм. Визнати той чи інший матеріал екстремістським (так само як збудливим міжнаціональну ворожнечу або, скажімо, порнографічним) можна, лише провівши експертизу. А до тієї пори поширення матеріалу захищено правом на свободу слова.

Розглянемо характерну слідову картину для злочинів даного виду.

Якщо розміщення інформації злочинець проводив особисто і вручну, сліди залежать від способу розміщення. При розміщенні інформації особисто, але з використанням автоматизації будуть також сліди від пошуку, настройки і пробних запусків відповідної програми. Існують загальнодоступні безкоштовні і платні програми для розсилки спаму по електронній пошті, по телеконференцій, для масового постінгу в веб-форуми і дошки оголошень.

При замовленні розміщення (розсилки) у спеціалізуються на цьому професіоналів, то є спамерів, шукати сліди розміщення на комп'ютері підозрюваного безглуздо. Краще шукати сліди його контактів зі спамерами: оголошення спамерів, листування з ними, телефонні переговори, сліди підготовки розміщується тексту, переказу грошей. Знайдені спамери, якщо їх схилити до співпраці, дадуть викривають свідчення, і ніяких технічних слідів розміщення інформації шукати вже не знадобиться.

Крім того, зловмисник напевно буде сам переглядати розміщені їм тексти як з метою контролю, так і заради відстеження реакції інших. У разі особистих некорисливих мотивів він повинен відчувати задоволення при перегляді своїх повідомлень. При перегляді утворюються відповідні сліди.

Розглянемо такий вид злочину, як DoS-атаки.

Проаналізуємо характерні особливості способу вчинення DoS-атак.

DoS-атака або атака типу «відмова в обслуговуванні» є одним з видів незаконного втручання, а саме такого, який призводить до блокування інформації і порушення роботи ЕОМ і їх мережі. Інші види незаконного втручання (копіювання інформації, знищення інформації), а

також використання шкідливих програм можуть бути етапами здійснення DoS-атаки.

Такі атаки прийнято розділяти на два типи: атаки, що використовують будь-які уразливості в атакується системі і атаки, які не використовують вразливостей. У другому випадку своєрідним «вражаючим чинником» атаки є перевантаження ресурсів атакується системи – процесора, ОЗУ, диска, пропускної здатності каналу.

Розглянемо характерні особливості кіберзлочинців, що вчиняють злочини даного виду.

В даний час зустрічаються DoS-атаки як з особистими, так і з корисливими мотивами. Ще 2-3 роки тому особисті мотиви переважали . Але зараз спостерігається чітка тенденція зростання числа DoSатак з корисливими мотивами – з метою вимагання або недобросовісної конкуренції.

Організувати DoS-атаку на типовий веб-сайт не представляє з себе складного завдання, вона під силу IT-фахівця середньої кваліфікації, що має в своєму розпорядженні середнє ж обладнання і середньої ширини канал зв'язку. Відповідно, на чорному ринку DoS-атака на звичайний веб-сайт коштує десятки доларів за добу. На більший або більш захищений об'єкт – перші сотні доларів за добу. Можливі оптові знижки. Замовити атаку може собі дозволити навіть один ображений індивідуум. Інструмент для здійснення розподілених DoS-атак – бот-мережі (ботнети) – також є у продажу на чорному ринку за порівняно низькою ціною, порядку десятків доларів за тисячу бот-хостів. І ціна ця останнім часом знижується.

З іншого боку, в Мережі з'являється все більше і більше чисто інформаційного бізнесу, благополуччя якого цілком і повністю залежить від доступності його сайту або іншого мережевого ресурсу. Це онлайн-магазини, онлайн-аукціони, онлайн-казино, букмекерські контори і деякі інші види підприємств. Зупинка роботи веб-сайту в таких умовах

означає повну зупинку бізнесу. Кілька тижнів простою можуть повністю розорити підприємство. Природно, при таких умовах перебувають бажаючі шантажувати власника і отримати з нього викуп за припинення DoS-атаки. Кілька років тому подібних підприємств (е-бізнесу) з істотними доходами ще не було. Відповідно, не було і DoS-вимагання.

Отже, можна виділити два типи злочинів, пов'язаних з DoS-атаками, - з метою завдати неприємностей власникові або користувачам атакується ресурсу і з метою отримати викуп. У першому випадку, як і при наклепі і образах, слід шукати «скривдженого». При цьому безпосереднім виконавцем може бути як він сам, так і найнятий професіонал.

У другому випадку ми маємо справу з холоднокровним кримінальним розрахунком, і злочин мало чим відрізняється від офлайнового вимагання або недобросовісної конкуренції.

Розглянемо обстановку вчинення злочину, характерну для DoS-атаки.

Один тип DoS-атаки заснований на використанні вразливостей в програмному забезпеченні, що атакується ресурсу. Інший тип – так званий флуд – не використовує ніяких вразливостей і розрахований на просте вичерпання ресурсів жертви (смуга каналу, оперативна пам'ять, швидкодія процесора, місце на диску тощо). Як легко зрозуміти, до флуду немає невразливих, оскільки будь-які комп'ютерні ресурси кінцеві. Тим не менше різні сайти схильні до флуду в різному ступені. Наприклад, CGI-скрипт, який працює на веб-сайті, може бути написаний не оптимально і вимагати для своєї роботи занадто багато оперативної пам'яті. Поки такої CGI-скрипт викликається раз в хвилину, ця не оптимальність зовсім непомітна. Але варто зловмисникові зробити виклик CGI-скрипта хоча б сто разів на секунду (ніяких особливих витрат з боку зловмисника для цього не потрібно, всього 300 пакетів в

секунду близько 5 Мбіт / с) – і не оптимальність CGI-скрипта призводить до повного паралічу веб-сайту.

Тобто запас по продуктивності і є первинний захист від DoS атаки.

Звичайні хостинг-провайдери тримають на одному сервері по кілька десятків клієнтських веб-сайтів. З економічних причин великого запасу продуктивності вони зробити не можуть. Звідси випливає, що типовий веб-сайт, розміщений у хостинг-провайдера, вразливий навіть до самого найпростішого флуду.

Розглянемо характерні особливості потерпілого від DoS атаки.

Потерпілим в переважній більшості випадків виступає юридична особа. Комерційні організації не часто бувають зацікавлені в офіційному розслідуванні, оскільки для них головне – усунути небезпеку і мінімізувати збитки. В покарання зловмисника вони не бачать для себе ніякої вигоди. А участь в судовому процесі в ролі потерпілого часто негативно відбивається на діловій репутації.

Виступити потерпілим організація-власник атакується ресурсу може в таких випадках:

– коли є впевненість, що ні покараний зловмисник буде повторювати атаки;

– коли підприємству треба звітувати за понесені збитки або перерви в наданні послуг перед партнерами, клієнтами, акціонерами;

– коли керівник підприємства вбачає в атаці особисті мотиви, особисту образу, коли уражене його самолюбство.

В інших випадках не доводиться розраховувати на зацікавленість потерпілого в розкритті злочину.

Слід пам'ятати, що багато DoS-атаки впливають відразу на цілий сегмент Мережі, на канал, на маршрутизатор, за яким можуть розташовуватися багато споживачів послуг зв'язку, навіть якщо

безпосередній метою атаки є лише один з них. Для цілей розслідування необхідно встановити, на кого саме був спрямований умисел злочинця.

А формальним потерпілим може виступити будь-який з постраждалих від атаки.

Замість формального потерпілого ми тут опишемо особливості особистості фахівця, який обслуговує атакувати інформаційну систему і відповідає за її захист. Розуміння його особистості допоможе зрозуміти причини і механізм скоєння злочину.

Типовий професійний системний адміністратор – людина, в реальному світі нічого з себе не представляє (навіть далеко не завжди високооплачуваний), але в світі віртуальному – цар і бог. двояке становище сильно сприяє розвитку комплексів неповноцінності і прагнення компенсувати в віртуальності свою нікчемність в реальному світі. Оскільки мова йде про молоду людину, значну частину часу вимушеному проводити за комп'ютером (інакше професіоналізм не придбати), даний комплекс часто посилюється статевої незадоволеністю. Тепер уявіть, що може накоїти такий системний адміністратор з болючим бажанням продемонструвати свою владу. За умови, що керівник компанії в технічних питаннях зовсім не розбирається або не цікавиться ними.

Як приклад можна навести DoS-атак на веб сайт, яка була замовлена одним з відвідувачів веб-форуму на ньому. Необережне слово, відповідна грубість, перепалка – в результаті адміністратор форуму закрив доступ користувачу, якого він вважав винним, і в подальшому видаляв всі його акаунти. Ображений вирішив помститися. Як з'ясувалося в ході розслідування, він замовив DoS-атаку на цей сайт. Атака була потужною, а сайт, сервер і мережу в цілому не були розраховані на великі навантаження, працювали поблизу межі своєї продуктивності. В результаті атаки вийшов з ладу не тільки цільової веб-сайт, але і кілька десятків веб-сайтів, які жили на тому ж сервері. А

також втратили працездатність сусідні сервера, що використали той же канал зв'язку. Постраждалими були: магістральний провайдер, у якого виявився цілком забитий флудом канал зв'язку, оператор дата-центру, кілька хостинг-провайдерів, чиї сервера були сусідами з цільовим, а також всі їх клієнти - всього більше сотні осіб.

DoS-атаки такого типу було б значно легше запобігти, ніж відобразити або подолати її шкідливі наслідки. Варто було адміністратору веб-форуму бути трохи стриманішими або хоча б замислитися про наслідки, і атаки вдалося б уникнути. Можна сказати, що для потерпілого від DoS-атаки (точніше, співробітників юридичної особи-потерпілого) характерно провокує поведінку в онлайнових взаєминах.

Розглянемо характерні особливості слідової картини DoS-атак.

При підготовці і проведенні DoS-атаки утворюються такі сліди технічного характеру:

– наявність інструментарію атаки – програмних засобів (агентів), встановлених на комп'ютері зловмисника або, частіше, на чужих використовуваних для цієї мети комп'ютерах, а також засобів для управління агентами;

– сліди пошуку, тестування, придбання інструментарію;

– логи (переважно статистика трафіку) операторів зв'язку, через мережі яких проходила атака;

– логи технічних засобів захисту – детекторів атак і аномалій трафіку, систем виявлення вторгнень, між мережевих екранів, спеціалізованих анті флудових фільтрів;

– логи , зразки трафіку та інші дані, спеці але отримані технічними фахівцями операторів зв'язку в ході розслідування інциденту, вироблення контрзаходів, відбиття атаки. (Слід знати, що DoS-атака вимагає негайної реакції, якщо власник бажає врятувати свій ресурс або хоча б сусідні ресурси від атаки. В ході такої боротьби обидві сторони

можуть застосовувати різні маневри і контрманевр, через що картина атаки стають більш складними);

– сліди від вивчення підозрюваним (він же замовник атаки) реклами виконавців DoS-атак, його листування, переговорів і грошових розрахунків з виконавцями;

– сліди від контрольних звернень підозрюваного до атакованого ресурсу в період атаки, щоб переконатися в її дієвості.

При професійному здійсненні атаки використовуються зомбі-мережі або інший спеціалізований інструментарій. Природно, він не одноразовий. Виконавці не зацікавлені в простоюванні своїх потужностей і можуть здійснювати кілька атак одночасно, або здійснювати тими ж програмними агентами паралельно з атакою інші функції, наприклад, розсилання спаму.

Розглянемо такий вид злочину, як дефейс.

Слушним удається розгляд характерних способів вчинення злочинів даного виду.

Дане правопорушення полягає в тому, що зловмисник тим або іншим способом змінює зовнішній вигляд публічного веб-сайту потерпілого, найчастіше його титульну сторінку. Технічно це можна здійснити, отримавши доступ на запис до директорії, де зберігаються дані вебсервера. Також часто дефейс виробляють, скориставшись вразливістю в самому веб-сервері або одному з його CGI-скриптів. Буває, що зловмисник змінює веб-сторінку, скориставшись штатної функцією, під аккаунтом одного із законних користувачів.

Слід відрізняти дефейс від підміни веб-сайту за допомогою атаки на DNS або зміни DNS-записи для сайту жертви. Це інший спосіб, хоча мета атаки може бути такою ж, як при дефейсі.

Явище це досить поширене. Фіксуються тисячі подібних інцидентів щомісяця. Можна припустити, що не всі дефейси

потрапляють в статистику, оскільки для власника зламаного веб вигідно приховати такий інцидент.

Розглянемо характерні риси кіберзлочинців, які вчиняють дефейси.

Мотиви для дефейса бувають такі (перераховані в порядку убування частоти):

– прагнення продемонструвати публічно свою кваліфікацію;

– політичні, релігійні, інші ідеологічні мотиви;

– особиста неприязнь, особистий конфлікт з потерпілим або ким-небудь з його працівників;

– прагнення дискредитувати власника веб-сайту, зіпсувати йому репутацію в цілях конкурентної боротьби, вплинути на його капіталізацію в цілях біржовий спекуляції;

– прагнення продемонструвати наявність уразливості в ПЗ, залучити до неї увагу.

Слушним удається розгляд характерних особливостей слідової картини дефейсу.

На зламаному комп'ютері слідів залишається небагато, зловмисник намагається по можливості знищити їх. Не слід дивуватися, якщо слідів там взагалі знайти не вдасться. Більше слідів можна знайти на комп'ютерах, які хакер використовує в якості проміжних вузлів для дослідження атакується веб-сайту і доступу до нього. Також знадобляться статистичні дані транзитних провайдерів. А на власному комп'ютері зловмисника слідів повинно бути ще більше – там повинні знайтися перероблена або заново виготовлена веб-сторінка, а також її проміжні варіанти, засоби для здійснення несанкціонованого доступу, засоби для пошуку і експлуатації вразливостей на цільовому веб-сайті та проміжних вузлах.

Крім цього, зловмисникові ще необхідно привернути суспільну увагу до дефейсу. В іншому випадку акція може залишитися

непоміченою – змінені сайти ніколи не залишається в такому стані, власник зазвичай швидко відновлює первісний вид.

Отже, зловмисник одразу після «злому» або незадовго до нього будь-яким способом сповістить світ про свій злочин.

Це можуть бути повідомлення по електронній пошті, стаття в телеконференції або на веб-форумі. Всі ці дії залишать додаткові сліди.

Зловмисник також буде періодично перевіряти результат дефейса і відслідковувати реакцію громадськості на нього. Ці дії він може здійснювати зі свого комп'ютера, без особливих заходів для анонімізації.

Розглянемо характерні особливості потерпілого від дефейсу.

Найчастіше потерпілим є юридична особа. Зазвичай підприємство-потерпілий не зацікавлене в розголошенні інформації про інцидент. Але якщо широкий розголос вже сталася, позиція потерпілого може змінитися, оскільки необхідно чимось компенсувати шкоди діловій репутації і якось виправдатися перед акціонерами і клієнтами. Швидко знайти і притягнути до відповідальності зловмисника – це все-таки деяка компенсація в плані репутації і громадських зв'язків.

До даного злочину відноситься все, сказане про потерпілих в попередньому розділі («DoS-атаки»).

Розглянемо криміналістичні особливості вчинення такого кіберзлочину, як створення шкідливих програм.

Слушним удається криміналістичний аналіз способу створення шкідливого програмного забезпечення.

Антивірусні аналітики відзначають явну тенденцію до комерціалізації шкідливого ПЗ. Ще 5-7 років тому майже всі віруси і черв'яки створювалися без явної корисливої мети, як вважають, з хуліганських спонукань або з честолюбства.

А серед сучасних шкідливих програм більшість складають програми, заточені під отримання вигоди . Основні їх різновиди (з точки зору призначення) суть наступні:

– троянські програми для створення зомбі-мереж, які потім використовуються для розсилки спаму, DoS-атак, організації фішерських сайтів тощо;

– нерідко вони забезпечені механізмом само розповсюдження;

– так зване spyware, тобто черви і троянці для викрадення персональних даних – паролів і ключів до платіжних систем, реквізитів банківських карток і інших даних, які можна використовувати для шахрайства або розкрадання;

– так зване adware, тобто шкідливі програми, таємно впроваджуються на персональний комп'ютер і показують користувачеві несанкціоновану рекламу (іноді до класу adware зараховують не тільки шкідливі, але і «законослухняні» програми, які показують рекламу з відома користувача);

– руткіти, службовці для підвищення привілеїв користувача і приховування його дій на «зламаному» комп'ютері;

– логічні бомби, які призначені для автоматичного знищення всієї чутливої інформації на комп'ютері в заданий час або при виконанні (при невиконанні) певних умов;

– так зване «ransomware» – підвид троянських програм, які після таємного впровадження на комп'ютер жертви шифрують файли, які містять призначену для користувача інформацію, після чого пред'являють вимога про сплату викупу за можливість відновлення файлів користувача.

2.2. Особливості розслідування перешкоджання роботі мереж електрозв'язку, комп'ютерних мереж, роботі комп’ютерів та автоматизованих систем, що вчиняються з корисливих мотивів

Слушним удається розгляд особливостей розслідування перешкоджання роботі мереж електрозв'язку, комп'ютерних мереж,

роботі комп’ютерів та автоматизованих систем, що вчиняються з корисливих мотивів.

Розглянемо криміналістичні особливості онлайн-шахрайства. Розглянемо типові способи вчинення онлайн-шахрайства. Така форма торгівлі, як інтернет-магазин, знайшла широке застосування серед бізнесменів з цілого ряду причин. Він, зокрема, відрізняється низькими витратами на організацію торгівлі. Вартість веб-сайту з відповідним бек-офісом не йде ні в яке порівняння з вартістю утримання реальної торгової площі. До того ж залежність поточних витрат інтернет-магазину від його обороту якщо і не дуже близька до пропорційної, то значно ближче до неї в порівнянні з магазином реальним. Це означає, що при відсутності (нестачі) покупців збитки будуть невеликі. Наприклад, ціна готового, стабільно працюючого інтернет-магазину починається з 15-20 тисяч доларів. У порівнянні з реальним (офлайнових) магазином, тим більше у великому місті, це просто смішні гроші.

Саме ця особливість інтернет-торгівлі привернула сюди шахраїв. Витративши відносно невелику суму, зловмисник може створити видимість нормального торговельного підприємства і зайнятися шахрайством або обманом споживачів. Десяток-другий жертв цілком окупають зроблені витрати. Для магазину на вулиці таке було б немислимо.

Однак, крім фіктивних інтернет-магазинів шахраї використовують і інші приводи для отримання платежів:

– псевдо-сайти благодійних організацій, релігійних організацій, політичних партій і рухів, які нібито збирають пожертви;

– спам-розсилки та сайти з проханням про матеріальну допомогу під зворушливу історію про бідну сирітку, жертві війни, заручника тощо;

– сайти фіктивних шлюбних агентств і окремі віртуальні нареченої;

– шахрайські онлайн «банки» і «інвестиційні фонди», які обіцяють величезні відсотки за вкладами;

– розсилки і сайти про нібито виявлені вразливості і чорних ходах в платіжних системах, що дозволяють множити свої гроші, наприклад, переславши їх на особливий рахунок (в тому числі шахрайства II порядку, побудовані на тому, що жертва думає, ніби вона обманює обманщика);

– шахрайські сайти і розсилки, що пропонують віддалену роботу (на таку найчастіше клюють мережеві ескапісти) і вимагають під цим приводом будь-якої «вступний внесок».

Все такі злочини мають одну і ту ж криміналістичну характеристику і зводяться до розміщення інформації в Мережі, анонімному взаємодії з жертвою і отримання від неї грошей з подальшим зникненням з Мережі.

Наприклад, онлайн-шахраї розсилають електронні листи, в яких жертвам пропонується перевести гроші за допомогою мережевої платіжної системи на певний рахунок. У шахрая є мінімум добу на те, щоб зібрати гроші без ризику отримати звинувачення в обмані. Фактично навіть більше: за допомогою заздалегідь підготовлених правдоподібних виправдань реально розтягнути термін до трьох діб. Тільки після цього адміністрація платіжної системи почне отримувати перші скарги на обман. Пропозиції розсилається за допомогою сучасних спамових технологій, масово одночасно. З близько мільйона розісланих копій будуть отримані від 2 до 4%. Якщо хоча б 1% осіб, які отримали лист, повірять в обман, шахраї заробить величезні кошти, які покриють всі витрати.

Типова обстановка вчинення злочину полягає у наступному. Такі особливості, як збереження анонімності власника веб-сайту або розсилки і великий проміжок часу між прийомом замовлення і його виконанням, дозволяють шахраям сподіватися на успіх свого своєї діяльності. Таким чином, відповідно до особливостей планування

кіберзлочинцями кримінальної діяльності слід, на нашу думку, виділити наступні групи ознак фіктивного інтернет-магазину:

– видима сильна економія на веб-сайті, рекламі, персоналі, послуги зв'язку і другом; шахрай замість повноцінного магазину обмежується одним лише «фасадом», дизайн сайту і товарний знак часто запозичені, замовлення обробляються явно вручну, не використовується банківський рахунок;

– прагнення приховати особу власника там, де вона повинна вказуватися, – при реєстрації доменного імені, придбанні послуг зв'язку, підключення телефонного номера, дачі реклами тощо;

– застосовуються тільки такі способи оплати, де можливо приховати особу одержувача платежу, неможлива оплата кур'єру при отриманні;

– період між замовленням товару і його доставкою максимально розтягнутий;

– відсутні дешеві товари.

Потерпілий по вказаній категорії справ як правило раніше вже користувався послугами інтернет-магазинів, є користувачем однієї з платіжних систем, які використовували шахраї.

Також потерпілому властиво до останнього моменту сподіватися, що його все-таки не обманули або це було зроблено ненавмисно. Навіть через рік деякі з ошуканих покупців все ще можуть повірити, що гроші їм повернуть. Наприклад, вже виявлено і затримано власника фальшивого онлайн-магазину. Відомий один з його клієнтів – той, який і звернувся в правоохоронців. Щоб знайти інших потерпілих, має сенс відновити роботу веб-сайту, на якому розміщувався шахрайський магазин і вивісити там оголошення з проханням до жертв шахрая звернутися до слідчого, який веде справу.

Слідова схема всіх онлайн-шахрайства виглядає наступним чином:

– розміщення (розсилка) інформації;

– взаємодія з жертвою;

– отримання грошового переказу.

Зазначені етапи передбачають залишення слідів технічного характеру. Хоча шахраї, очевидно, будуть намагатися вжити заходів для своєї анонімізації. Щодо отримання грошей шахраїв крім анонімізації рятує швидкість: переклад отриманих коштів між різними платіжними системами здійснюється досить швидко, але вимагає багато часу для відстеження.

При розміщенні шахраями підробленого інтернет-магазину можна розраховувати на виявлення наступних видів слідів:

– реєстраційні дані на доменне ім'я; логи від взаємодії з реєстратором доменних імен; сліди від проведення платежу цього реєстратору;

– сліди при налаштуванні DNS-сервера, що підтримує домен шахраїв;

– сліди від взаємодії з хостинг-провайдером, у якого розміщений веб-сайт: замовлення, оплата, настройка, заливши контенту;

– сліди від рекламування веб-сайту: взаємодія з рекламними майданчиками, системами банерообміну, розсилка спаму;

– сліди від відстеження активності користувачів на сайті.

При взаємодії з жертвами обману шахраї залишають такі сліди:

– сліди при прийомі замовлень - по електронній пошті, по ICQ, через вебформу;

– сліди від листування з потенційними жертвами.

При отриманні грошей шахраї залишають такі сліди:

– сліди при здійсненні введення грошей в платіжну систему (реквізити, які зазначаються жертві);

– сліди при перекладі грошей між рахунками, які контролюються шахраями;

– сліди при виведенні грошей;

– сліди від дистанційного керування шахраями своїми рахунками, їх відкриття і закриття;

– сліди від взаємодії шахраїв з посередниками по відмиванню і переведення в готівку грошей.

Розглянемо криміналістичні особливості кіберзлочинців, які створюють та розповсюджують шкідливе програмне забезпечення.

Як сучасна шкідлива програма є лише засобом, технологічним елементом для кримінального бізнесу, так і сучасний «автори» програм-вірусів працює не сам по собі, а виконує замовлення інших. Це може бути пряме замовлення, коли програміст-вірмейкерів отримує технічне завдання, виконує його і віддає готовий продукт замовнику. Це може бути непрямий замовлення, коли вірмейкерів, знаючи потреби чорного ринку, намагається їх задовольнити своїм продуктом, який потім і реалізує (ліцензує користувачам) самостійно.

Давно не відзначалося випадків, коли одна людина виконувала весь злочинний задум цілком – писав шкідливу програму, застосовував її, використовував результат застосування для отримання прибутку.

Таким чином, творець шкідливої програми – це майже завжди член злочинної групи. Його діяльність не має сенсу у відриві від замовників і користувачів шкідливої програми.

Крім створення шкідливих програм кримінальним злочином і їх застосування. Особа, що використовує таку програму, теж в більшості випадків не реалізує результати своєї праці безпосередньо, а продає або передає їх далі, іншим членам злочинної групи.

Нарешті, третій тип – це реалізатори результатів застосування шкідливих програм, тобто спамери, вимагачі, кардери, шахраї.

Наведемо приклади типових кримінальних «колективів».

1. Спамери.

Перший спільник створює і вдосконалює програмне забезпечення для таємного впровадження на комп'ютери користувачів (троянці).

Другий, купивши у першого право на використання зазначеної програми, розсилає її в масовому порядку, приймає сигнали і враховує примірники, успішно впроваджених троянців, об'єднує їх в структуровану зомбі-мережа. Готову мережу (цілком або частково, назовсім або на час) він продає третього спільника, який з її допомогою здійснює розсилку спаму. Замовлення на розсилки приймає четвертий спільник, який шукає замовників за допомогою того ж спаму, частина отриманих від замовників грошей перераховує третього в оплату його послуг. П'ятий займається збором і верифікацією адрес електронної пошти для розсилок. Зібрані бази адрес (або підписку на такі бази) він продає або четвертому, якій третій спільникові.

2. Кардери. Перший з спільників (точніше, перша група, одну людину тут не вистачить) займається збором атрибутів банківських карт. Він може служити продавцем або офіціантом і непомітно знімати дані з карток клієнтів. Він може бути менеджером у фірмі або банку і отримувати доступ до бази даних карток в силу службового становища.

Він може отримувати номери карток, впроваджуючи шкідливі програми-шпіони (spyware) або через фішинг. Здобувши кілька номерів (або навіть дампов) банківських карт, перший спільник збуває їх другого. Другий виконує роль організатора кримінального бізнесу. Він акумулює у себе дані і розподіляє їх виконавцям.

Третій спільник виконує на замовлення другого верифікацію реквізитів карт, тобто перевіряє їх дійсність і придатність для платежів. Четвертий спільник створює і підтримує платний веб-сайт або фіктивний магазин або інтернет-казино з можливістю оплати послуг картками.

Він має кілька договорів з білінговими компаніями, час від часу змінює їх, а також свою вивіску . Це механізм для відмивання грошей. П'ята група спільників отримують від другого партії номерів банківських карт по кілька десятків і вводять їх через підприємство,

призначене для «відмивання» коштів четвертого спільника під виглядом різних клієнтів. При цьому вони повинні за допомогою технічних засобів емулювати доступ з різних країн і з різних комп'ютерів. За свою роботу вони отримують відрядну оплату, рідше – відсоток з доходів. Шостий спільник є інший канал реалізації, він займається так званим речовим кардингом. Отримуючи від другого «добірні», найбільш перспективні номери кредиток, він використовує їх для покупок в справжніх інтернет-магазинах. Купується в основному дорога, легка і ліквідна техніка – мобільні телефони, відеокамери, комп'ютерні комплектуючі, деякі автозапчастини тощо.

Природно, замовляються вони зовсім не на його адресу. Для отримання замовлень існує сьома група спільників – дроп. Це громадяни з благополучних країн, оскільки більшість інтернет-магазинів не доставляють замовлення поза США, Канади та ЄС, а якщо і доставляють, то перевіряють таких покупців дуже ретельно. Робота дропов полягає в тому, щоб підтвердити по телефону співробітнику магазину, що замовлення зробив він, отримати посилку і тут же переслати її шостому спільникові (іноді – іншому дроп, для більшого заплутування слідів). Дроп вербуються десятками з малозабезпечених верств суспільства типу студентів.

Зазвичай дроп виконує всього десяток-другий операцій з інтервалом в кілька тижнів. Він отримує оплату відрядно або у вигляді відсотка від вартості товару. Нарешті, восьмий спільник займається отриманням і реалізацією посилок від дропів.

3. Фішери. Перший спільник займається розміщенням підроблених веб-сайтів банків та інших установ. До складу програм такого сайту входить система для моментальної відсилання введених клієнтом конфіденційних даних зловмисникові, природно, не безпосередньо, щоб важко було його обчислити. Другий виготовляє ці сайти, становить підроблені листи і розсилає їх, але не самостійно, а

користуючись для цього послугами спамерів. Третій спільник займається реалізацією отриманих даних (номера карт з пін-кодами або паролі до платіжних систем) кардерам або іншим кримінальним структурам. Буває, що реалізацією пін-кодів злочинна група займається самостійно. Тоді передбачений четвертий спільник, який виготовляє «пластик», тобто копії банківських карт для офлайнових магазинів і банкоматів, а також п'ята група, яка власне знімає з банкоматів гроші, отримуючи для цього карти і пін-коди у четвертого.

Видно, що шкідливе ПО у всіх випадках грає роль інструменту для одного з етапів великого злочинного задуму. І творець, і застосувачів шкідливих програм також виконують загальний задум.

Отже, ймовірний злочинець у справах про створення та використання шкідливих програм – це учасник злочинної групи, що працює в цій групі на основі найму або за відсоток від доходу або як самостійний творець знарядь злочину. Тобто з точки зору економіки «автор» вірусів продає в одних випадках свою робочу силу, в інших – свою працю, а по-третє – результат своєї індивідуальної праці.

Як правило, це професійний програміст, встає на злочинний шлях вже після вибору професії. Його рушійним мотивом є гроші. Мотиви, характерні для типу «хакер», тобто самоствердження і дослідницький інтерес, можуть мати значення лише на першому етапі, при залученні його в злочинну діяльність. Корисливий же мотив – завжди основний.

Розглянемо криміналістичні особливості створення програм-«діалерів».

Одним з видів шахрайства є несумлінне використання платних телефонних ліній. Абонований відповідний номер з високою оплатою за «розмова» з боку абонента, шахраї усілякими способами намагаються спровокувати виклики на нього з боку абонентів. Поміщають цей номер в завідомо неправдивої рекламі, відправляють SMS і роблять вихідні дзвінки з цього номера, щоб абонент передзвонив, самі здійснюють

дзвінки на свій номер, користуючись недосконалістю білінгу оператора, нав'язують помилкову інформацію про виклики телефонної мережі, а також вставляють (завантажують) цей номер під шкідливі програми-діалери (dialer), які змушують модем користувача здійснювати виклик.

За умовами договору оператор абонента платить за такий дзвінок оператору абонента, а потім намагається отримати гроші зі свого абонента.

Наведемо більш детально один з найпоширеніших типів такого шахрайства – з використанням шкідливої програми-діалери. Більшість дзвонилок відносяться до класу троянських програм. Одні з них мають звичайний для троянців механізм таємного впровадження на комп'ютер або маскуються під корисні програми. Інші таких механізмів не мають і розраховані на одноразовий запуск самим користувачем, який введений в оману методами соціальної інженерії.

Наприклад, на веб-сайті, що містить численні посилання на порнографію, деякі посилання ведуть на таку програму з поясненням «запустіть для перегляду відео». Обдурений користувач клікає на гіперпосилання, тим самим завантажуючи програму-звонилку, і запускає її. Будучи запущеної, вона таємно впроваджується на комп'ютер користувача (можливо, при цьому навіть показує йому відео) і згодом активізується, набираючи за допомогою модему платний номер. Зловмисники отримують через оператора гроші за досконалий дзвінок, а потерпілому потім надається розбиратися зі своїм оператором зв'язку, доводячи, що він не дзвонив в Ліхтенштейн і не отримував послугу «для дорослих».

Слід зауважити, що серед подібних програм-діалерерів є і нешкідливими, які не приховують своєї присутності і свого призначення і показують користувачеві, який дзвінок і за яким тарифом буде проведений. Вони також іноді використовуються для обману

споживачів, але не викликають стільки проблем у абонентів і не тягнуть звинувачення в шахрайстві і у використанні шкідливих програм.

Отже, більшість програм-діалерів є шкідливими, оскільки впроваджуються на комп'ютер і виробляють свої без вашого відома користувача і дозволи від нього. Багато потерпілих наполягають на порушенні кримінальної справи за фактом зараження такою програмою, оскільки вважають, що це дозволить їм не оплачувати вартість дзвінка оператору зв'язку.

Але на сьогоднішній день суди не визнають шкідливі програми стихійною силою, а їх дії – форс-мажорними обставинами.

Тому що заразилися такими програмами користувачам все ж доводиться оплачувати дзвінки. Втім, іноді оператор зв'язку схильний «прощати» таку заборгованість абонента – не за законом, а по справедливості.

Одні з програм-діалерів мають власний механізм поширення, найчастіше розсилають себе по електронній пошті за списком адрес, знайдених на зараженому комп'ютері. Інші самостійно поширюватися не вміють, і зловмисник змушений розміщувати їх на веб-сайтах, маскувати під щось невинне і рекламувати свій сайт.

Кількість заражень подібними програмами повільно знижується, оскільки все менше комп'ютерів використовують модем, все більше – виділені лінії зв'язку.

Розглянемо типову слідову картину використання програм-діалерів.

При виготовленні шкідливих програм можна виявити наступні цифрові сліди:

– вихідний текст шкідливої програми, його проміжні варіанти, вихідні тексти інших шкідливих або подвійного призначення програм, з яких «автор» вірусної програми запозичив фрагменти коду;

– антивірусне ПЗ різних виробників, на якому творець шкідливої програми обов'язково тестує свою, а також кошти для дизассемблювания і налагодження;

– програмні засоби для управління шкідливими програмами (багато з них працюють за схемою «клієнт-сервер», одна з частин впроваджується на комп'ютер жертви, а інша частина працює під безпосереднім керівництвом зловмисника); засоби і сліди тестування роботи шкідливих програм під різними варіантами ОС;

– сліди контактування з замовниками або користувачами шкідливої програми, передачі їм примірників і документації, оплати.

При поширенні та застосуванні шкідливих програм м можна виявити наступні цифрові сліди:

– засоби і сліди тестування роботи шкідливої програми під різними варіантами ОС;

– контакти з творцем або розповсюджувачем-посередником шкідливої програми

– програмні засоби для управління шкідливою програмою, дані про впровадження цієї програми до жертв, результати діяльності (паролі, звіти про готовність, викрадені персональні дані);

– засоби поширення шкідливої програми або контакти з тими, хто підрядився її поширювати.

Крім того, на комп'ютері жертви повинна знайтися сама шкідлива програма (її серверна або клієнтська частина). Дуже часто виявляє її сам потерпілий за допомогою антивірусного ПО. При цьому шкідлива програма може бути знищена по команді користувача або автоматично, відповідно до настройками антивіруса. Хоча виконуваний код шкідливої програми, виявлений в ході експертизи, є доказом у справі, у разі його знищення потерпілим без цього докази можна обійтися.

Лог антивіруса, а також сліди діяльності шкідливої програми, будучи досліджені в ході експертизи, дозволять експерту категорично

стверджувати, що на досліджуваному комп'ютері була встановлена певна шкідлива програма, хоча виконуваного коду цієї програми і не виявлено. Краще доручити таку експертизу підприємству, яке виробляє або обслуговує відповідну антивірусне ПЗ.

Розглянемо особливості розслідування кардерства.

Перш за все удається за доцільне розглянути способи вчинення кардерства.

Кіберзлочини, пов’язані з банківськими картами, вчиняються в кілька етапів. На першому етапі дані про банківські картки виходять різноманітними способами. На другому етапі вони сортуються, перевіряються, класифікуються, можливо, проходять через оптових посередників (скупка в роздріб, продаж оптом, продаж в роздріб). На третьому етапі дані банківських карт реалізуються, тобто конвертуються в гроші.

Зазначений ланцюжок ніколи не виконується однією людиною. Кожен з етапів пов'язаний зі своїми особливими навичками, досвідом у відповідній області, службовим становищем, доступом до техніки. Тому кримінальна ланцюжок завжди включає не менше трьох спільників.

Удається за доцільне розглянути окремі етапи вчинення кіберзлочинів з використанням банківських карток.

1. Отримання банківських карток та відомостей про них.

Перелічимо набори даних банківських карт, які представляють цінність:

– номер, термін дії, ім'я власника, код1 cvv або cvv2;
– дамп карти;
– дамп + пін-код.

Третій варіант – найпривабливіший для кардерів. Цей набір даних можна конвертувати в готівку найшвидшим способом і отримати при цьому максимальну суму.

Розглянемо способи отримання даних банківських карт:

– дистанційний неправомірний доступ до сервера, на якому такі дані зберігаються або обробляються, наприклад, до сервера магазину або банку – спосіб, найбільш часто передбачуваний недосвідченими людьми, але дуже не часто зустрічається на практиці;

– доступ до таких даних з використанням свого службового становища і недоліків в системі захисту інформації підприємства – дуже часто власники конфіденційної інформації роблять зайві заходи захисту від зовнішніх загроз, але нехтують захистом від загроз внутрішніх;

– не часто перехоплення інтернет-трафіку, коли дані карти передаються в відкритому вигляді (по протоколу HTTP або по електронній пошті);

– отримання даних банківських карт, або зняття дампа при обслуговуванні клієнтів в підприємствах торгівлі та харчування – схожий на попередній спосіб спосіб, але особливість в тому, що інформація копіюється безпосередньо з карти при фізичному контакті з нею;

– виманювання даних карт і іноді пін-кодів у власників методами фішингу;

– отримання дампов і пін-кодів за допомогою фальшивих банкоматів або приставок до банкоматів (скімінг);

– отримання самої картки шахрайським способом («ліванська петля» та ін.);

– звичайна крадіжка карти в її власника (буває, що пін-код записаний на ній або на листку, що лежить в тому ж гаманці).

Розглянемо криміналістичні особливості реалізації незаконно отриманих коштів, отриманих від вчинення кіберзлочинів з банківськими картками.

Реалізація даних з банківських карт, тобто звернення їх в гроші, може здійснюватися такими способами:

– речовий кардинг – придбання в інтернет-магазинах або в реальних магазинах (при наявності дампа карти) ліквідних товарів, частіше на продаж, рідше на замовлення, подальша їх реалізація;

– вчинення фіктивних покупок в інтернет-магазинах або придбання послуг платних сайтів за змовою з їх власниками; за допомогою

– даних чужий карти проводиться оплата, білінгове підприємство (воно не бере участі в змові) враховує платіж і переводить магазину за вирахуванням своєї комісії, магазин переводить обумовлену частку кардеру;

– гра в інтернет-казино; найняті кардером гравці реєструють в інтернет-казино багато акаунтів на ім'я власників карт, вносять з карт депозит, грають, а потім для тих акаунтів, де утворився виграш, проводять процедуру виведення коштів;

– використання інших інтернет-сервісів, де можливе отримання грошей, наприклад, організують показ аматорського відео;

– вимагання у магазина, банку, іншого підприємства, який несе відповідальність за збереження даних; за втрату і розголошення даних про карти клієнтів підприємство може піддатися санкціям з боку платіжної системи, отримати великий шкоди діловій репутації, може стати відповідачем за позовами клієнтів - за позбавлення від цих неприємностей багато хто готовий заплатити кардерам-здирникам;

– переведення в готівку в банкоматах; коли є дамп карти і пін-код, то виготовляється тверда копія карти (так званий «білий пластик», тому що зовнішнє оформлення для банкомату не потрібно), з якої в банкоматах знімається максимально можлива сума за мінімально можливий час.

Розглянемо криміналістичні особливості перерахованих способів придбання і реалізації даних банківських карт.

1. Скімінг.

Найбільш ласий шматок для кардерів – це повна копія (дамп) магнітної смуги карти разом з її пін-кодом. Такі дані дозволяють

отримати) доступ до пін-кодами клієнтів, не завжди витримують спокусу зв'язатися з кардерами і спільно очистити клієнтські рахунки.

У 1980-х і 1990-х була популярна установка фальшивих банкоматів і торгових терміналів. Багато з них навіть видавали клієнтам гроші або товари. Нині такі банкомати зустрічаються рідше.

Більш поширені «приставки» до легальних банкоматів, які непомітно для клієнта зчитують дані з магнітної смуги і «підглядають» введення пін-кодів.

Про поширеність подібного способу говорить те, що виробники банкоматів зараз передбачають в картоприймач механізм для нерівномірного протягування карти. Карта втягується в банкомат і екстрагується з банкомату ривками, щоб утруднити зчитування магнітної смуги можливим шпигунським пристроєм. Втім, у відповідь технічні заходи вже придумані.

2. Використання казино.

Для виплати грошей інтернет-казино вимагає підтвердження особи гравця, а також користується тільки неанонімні системами платежів. від гравця, побажав отримати виплату, швидше за все, зажадають надіслати скан-копію паспорта та будь-якого документа, що підтверджує місце проживання, наприклад, квитанції про оплату комунальних послуг. Можливо, від гравця зажадають отримати номер телефону заради додаткового підтвердження його особистості. Виплата проводиться на іменний банківський рахунок (при цьому не всякий банк буде визнаний благонадійним) або за допомогою іменного чека, який відправляється з поштою. Загалом, онлайн-казино виробили ряд процедур, які спрямовані на боротьбу з онлайн-шахрайством.

Кардери у відповідь винайшли контрзаходи. Чимало «спеціалістів» пропонують послуги з виготовлення скан-копій паспортів та інших документів за розумну ціну, телефонні номери в «благонадійних» країнах з перекладом вхідних дзвінків на будь-який

номер в будь-якій країні, банківські рахунки, що приймають платежі, адресовані довільним фізичним особам, і інші подібні послуги.

Також спостерігається поділ праці в області роботи з самими інтернет-казино. Реєстрацію акаунтів гравців зазвичай доручають окремим людям. На чорному ринку кардерських товарів і послуг продаються і купуються такі акаунти, як порожні, так і вже «відіграні», то є готові для виведення грошей.

3. Фіктивні покупки.

Типовий інтернет-магазин або платний веб-сайт для отримання платежів від своїх клієнтів використовує послуги так званого білінгових підприємства – фінансової установи, яка приймає дані банківських карт, здійснює транзакції і переводить отримані гроші (за вирахуванням своєї комісії) на банківський рахунок інтернет-магазину. У билинговой фірми є власна служба безпеки, що перешкоджає проведенню шахрайських операцій. Саме тому банки відмовляються працювати з дрібними онлайн-магазинами безпосередньо і вважають за краще взаємодіяти саме з білінгових підприємствами-посередниками. Білінгових підприємство відмовляє в обслуговуванні тим онлайновим магазинам, у яких відсоток відкликаних транзакцій (chargeback) перевищує деякий рівень, зазвичай 1%. Може відмовити в обслуговуванні і з іншої причини, якщо вважатиме інтернет-магазин підозрілим.

Веб-сайт типового онлайн-магазину навіть не має інтерфейсу для введення платіжних реквізитів. Відвідувач веб-сайту вводить їх прямо на веб-сторінці билинговой фірми, природно, користуючись захищеним (HTTPS) з'єднанням.

Один із способів реалізації даних банківських карт полягає в змові між кардером і власником онлайнового магазина. Часто такі магазини або платні веб-сайти влаштовуються спеціально заради прийому платежів по чужим картам. Спільники разом намагаються

обдурити білінгових підприємство, зробити так, щоб повернень було не більше встановленої кількості.

Для введення реквізитів карт в інтерфейс билинговой системи зазвичай наймаються окремі люди, набівщікі. Це «чорнороби» кардерського світу. Проте від них вимагається володіти певними навичками. Набівщік повинен використовувати для кожної нової карти новий проксі-сервер або сокс-сервер, бажано, розташований в тій країні, в якій живе власник картки. Він повинен потурбуватися, щоб його комп'ютер відповідав типовою конфігурації комп'ютера клієнта. При взаємодії з веб-інтерфейсом билинговой системи браузер користувача повідомляє наступні дані:

– марка і версія браузера;
– мову браузера;
– версія ОС;
– дозвіл екрана;
– сприймаються типи даних;
– сприймаються мови;
– сприймаються кодування даних;
– referrer, тобто адреса веб-сторінки, з якої користувач перейшов на дану веб-сторінку;
– деякі інші налаштування.

Зрозуміло, що якщо під час такої взаємодії передаються реквізити банківської картки Джона Сміта з США, а мова браузера виставлений український, то система запідозрить недобре. Також виникне підозра, якщо з одного і того ж IP-адреси будуть введені карткові реквізити двох різних людей з різних країн.

Тому набівщікі отримують необхідні інструкції та, якщо треба, ПО для своєї роботи. Саме через нашестя кардерів стали з'являтися альтернативні системи оплати послуг в Інтернеті. Деякі платні веб-сайти

вже не приймають банківських карт. Оплата здійснюється через телефонний дзвінок по платній лінії або іншим подібним способом. У таких способів більше накладні витрати, але це дешевше, ніж постійно вирішувати проблеми, створювані через кардинг.

4. «Реальний пластик».

На кардерських жаргоні «реальним пластиком» іменуються повноцінні тверді копії банківських карт. На них повинен бути присутнім кольоровий малюнок, голограма, бути ембосовану (видавлені) ім'я власника і магнітна смуга з потрібними даними.

Для цього способу реалізації потрібно дамп карти. Пін-код не потрібен. За дампи виготовляється тверда копія карти. Вона повинна не тільки нести вірні дані на магнітній смузі, але і виглядати відповідно. Малюнок карти, звичайно, не повинен збігатися з оригінальним, але він повинен бути присутнім і бути хорошої якості: чи не змащувати, чи не відшаровуватися. Бажано, щоб назва банку і карти відповідало коду (перші 6 цифр номера карти); втім, продавці рідко звертають на це увагу.

До такої підробленої мапі реалізатора бажано мати підроблений документ. Продавець або касир не зобов'язаний питати у покупця при собі посвідчення особи, але може це зробити, якщо виникнуть підозри. А вони, швидше за все, виникнуть, оскільки кардер з «реальним пластиком» піде купувати не корзинку продуктів в супермаркеті, а товари з великою цінністю що можна буде перепродати хоча б за 40-50% вартості. Здійснити багато покупок за підробленою карті не вдасться, одна, дві, може бути, три – і власник карти схаменеться і заблокує її.

У багатьох випадках що фальшивий документ виготовляють на ім'я власника карти. Це надійніше, але дорожче. Адже підроблена карта може бути використана не більше 2-3 разів. Після цього вона в кращому випадку буде заблокована, а в гіршому – потрапить в стоп-лист. Відповідно, і підроблений документ потрібно буде викинути разом з

картою. Інший варіант – «постійний» документ, разом з яким можна використовувати кілька різних карт. Відповідно до ім'ям в документі наноситься (ембосується) ім'я на карті. Тобто ім'я на карті буде відповідати документу, але не буде відповідати імені на магнітній смузі. В цьому випадку витрати нижче, але вище ризик, оскільки продавець може порівняти ім'я на чеку і ім'я на карті.

Зразок ж підписи на підробленою карткою можна намалювати такий, який зручно.

Пластикові заготовки для банківських карт, устаткування для нанесення зображень, ембосування і записи магнітної смуги є у вільному продажу. Але купувати його доцільно, тільки якщо збираєшся виготовляти карти сотнями. Одиничні екземпляри вигідніше замовляти на стороні. Повний виготовлення банківської карти на чорному ринку обійдеться в 100-200 доларів.

5. «Білий пластик».

Карта, що має тільки записану магнітну смугу, іменується у кардерів «білим пластиком». Її виготовлення обходиться зовсім недорого. Однак область використання обмежена лише банкоматами. Зрозуміло, необхідно знати пін-код. Набір дамп карти + пін-код коштують на чорному ринку дорого, проте з його допомогою можна вичавити картковий рахунок насухо, знявши в банкоматі весь залишок і весь кредитний ліміт.

Багато банків ставлять обмеження для банкоматних транзакцій – по географії, по максимальній сумі за раз і по максимальній сумі за день. Це дещо ускладнює кардерам життя. Карту можуть встигнути заблокувати і занести в стоп-лист, поки ще не всі гроші з неї зняті.

Крім реалізації в банкоматах можливі варіанти покупки товарів за «білого пластику» в магазинах. Природно, лише за змовою з продавцем.

6. «Посередницькі онлайн-сервіси».

Інструментом кардера може стати майже будь-який інтернет-сервіс, де передбачена виплата грошей клієнтам.

Деяке поширення мають посередницькі послуги з обміну відео. Суть їх полягає в тому, що одні користувачі бажають транслювати відеозображення через Інтернет, а інші бажають його споживати. (Зрозуміло, як правило, мова йде про еротичному відео, але посередник вважає за краще про це «не знати».) Посередник організовує цей процес, зводить покупця з продавцем і здійснює розрахунок між ними. Собі бере відсоток за посередництво Оскільки від покупців приймаються платежі за банківськими картками, а виплати продавцям здійснюються чеком або банківським переказом, є можливість «відмивання». Кардер реєструється на такому посередницькому сайті як покупець, як продавець і починає продавати послуги самому собі.

Це також не простий шлях. Служби безпеки знають, як привабливі для кардерів подібні сервіси, і всіляко намагаються перешкодити. Виплати обставляються різними умовами на зразок інтернет-казино. Кардери, зрозуміло, знаходять відповідні заходи.

Розгляд проблемних питань, щодо особливостей розслідування окремих видів перешкоджання роботі мереж електрозв'язку, комп'ютерних мереж, роботі комп’ютерів та автоматизованих систем, дає можливості зробити наступні висновки:

1. Спосіб вчинення наклепу, образ та екстремістські дії в глобальній комп’ютерній мережі Інтернет полягає, як правило, в розміщенні на загальнодоступному, як правило, популярному ресурсі в Інтернеті образливих, наклепницьких або екстремістських матеріалів.

2. Ресурси вчинення наклепу, образ та екстремістські дії в глобальній комп’ютерній мережі Інтернет можуть бути наступними: веб-форуми і дошки оголошень, веб-сторінки, повідомлення в телеконференціях (newsgroups), масова розсилка (спам) електронною

поштою, СМС-повідомленнями та іншими системами обміну повідомленнями. Інші засоби вживаються нечасто.

3. DoS-атака або атака типу «відмова в обслуговуванні» є одним з видів незаконного втручання, а саме такого, який призводить до блокування інформації і порушення роботи ЕОМ і їх мережі. Інші види незаконного втручання (копіювання інформації, знищення інформації), а також використання шкідливих програм можуть бути етапами здійснення DoS-атаки.

4. Організувати DoS-атаку на типовий веб-сайт не представляє з себе складного завдання, вона під силу IT-фахівця середньої кваліфікації, що має в своєму розпорядженні середнє ж обладнання і середньої ширини канал зв'язку.

5. Один тип DoS-атаки заснований на використанні вразливостей в програмному забезпеченні, що атакується ресурсу. Інший тип – так званий флуд – не використовує ніяких вразливостей і розрахований на просте вичерпання ресурсів жертви (смуга каналу, оперативна пам'ять, швидкодія процесора, місце на диску тощо).

6. Дефейс полягає в тому, що зловмисник тим або іншим способом змінює зовнішній вигляд публічного веб-сайту потерпілого, найчастіше його титульну сторінку. Технічно це можна здійснити, отримавши доступ на запис до директорії, де зберігаються дані вебсервера. Також часто дефейс виробляють, скориставшись вразливістю в самому веб-сервері або одному з його CGI-скриптів. Буває, що зловмисник змінює веб-сторінку, скориставшись штатної функцією, під аккаунтом одного із законних користувачів.

7. Однак, крім фіктивних інтернет-магазинів шахраї використовують і інші приводи для отримання платежів:

– псевдо-сайти благодійних організацій, релігійних організацій, політичних партій і рухів, які нібито збирають пожертви;

– спам-розсилки та сайти з проханням про матеріальну допомогу під зворушливу історію про бідну сирітку, жертві війни, заручника тощо;

– сайти фіктивних шлюбних агентств і окремі віртуальні нареченої;

– шахрайські онлайн «банки» і «інвестиційні фонди», які обіцяють величезні відсотки за вкладами;

– розсилки і сайти про нібито виявлені вразливості і чорних ходах в платіжних системах, що дозволяють множити свої гроші, наприклад, переславши їх на особливий рахунок (в тому числі шахрайства II порядку, побудовані на тому, що жертва думає, ніби вона обманює обманщика);

– шахрайські сайти і розсилки, що пропонують віддалену роботу (на таку найчастіше клюють мережеві ескапісти) і вимагають під цим приводом будь-якої «вступний внесок».

ВИСНОВКИ

Розгляд проблемних питань, пов’язаних із особливостей розслідування окремих видів перешкоджання роботі мереж електрозв'язку, комп'ютерних мереж, роботі комп’ютерів та автоматизованих систем, дає можливість зробити наступні висновки:

1. Основною мотивацією хакерів є: дослідницький інтерес, цікавість, прагнення довести свої можливості, честолюбство. Засоби захисту комп'ютерної інформації, її недоступність вони сприймають як виклик своїм здібностям. Характерними є хороші знання в області IT і програмування. Однак зустрічаються хакери, серед яких середній рівень знань виявився невисокий.

2. Для окремої категорії хакерів, так званих «script kiddies». Характерно те, що керуються тими самими мотивами, але не в змозі придумати своє і тому просто бездумно використовують готові інструменти, зроблені іншими.

3. Більш поширеним типом комп'ютерного зловмисника є «інсайдер» – людина, не занадто добре володіє знаннями в області IT, зате володіє доступом в інформаційну систему (ІС) в силу службового становища. Більша частина «зламів» комп'ютерних систем відбувається зсередини.

4. При розслідуванні незаконного втручання «інсайдер» – перша версія, яку слід розглядати. Навіть якщо неправомірний доступ був явно зовні, швидше за все, він став можливим через змову з місцевим співробітником. Якщо для «зовнішнього» хакера виявити вразливість в інформаційній системі являє собою завдання, то для співробітника підприємства майже всі уразливості видно з самого початку.

5. «Білий комірець» являє собою давно і добре відомого казнокрада, який змінив «інструменти» своєї діяльності на комп'ютер. Вкрасти у держави або у приватній компанії можна багатьма способів.

Крім банального розкрадання тут можливі хабар, комерційний підкуп, незаконне використання інформації, що становить комерційну таємницю, різні види шахрайства тощо.

6. На відміну від «інсайдера», «білий комірець» має мінімальну кваліфікацію в сфері IT і комп'ютер як знаряддя вчинення злочину не використовує. Комп'ютер тут виступає лише як носій слідів, доказів вчинення злочину.

7. «Е-бізнесмен» як тип кіберзлочинців не є кваліфікованим IT-спеціалістом і не має службового становища, яким можна зловжити. З самого початку вони планують саме створення фіктивного підприємства, створеного саме для вчинення злочинів, відмінно усвідомлюючи його протизаконність.

8. Рішення вчинити правопорушення саме в комп'ютерному (мережевому) середовищі, а не в офлайні «е-бізнесмени» приймають не через наявність особливих знань в цій області і не через внутрішню тягу до комп'ютерів, а виключно на основі раціонального аналізу. Вони порахували, що так їм буде «вигідніше».

9. «Антисоціальні типи» як тип кіберзлочинця відзначаються як інтернет-шахраї, які керувалися не тільки отриманням прибутку. Більш того, їх злочинний дохід часто бував менше, ніж середня зарплата фахівця тієї ж кваліфікації. Мотивом для скоєння шахрайства була антисоціальна психопатія (соціопатія) таких осіб і їх патологічна тяга до ведення подібних «ігор».

10. Суспільна небезпечність кіберзлочинів залежить, на думку автора, від наступних факторів:

– вид і розмір збитку. Очевидно, що більш суспільно небезпечними є ті з комп'ютерних злочинів, які мають на увазі насильство (в порівнянні з тими, які лише завдають матеріальної шкоди). Також більш пріоритетними є злочини, які посягають на права неповнолітніх та інших менш захищених суб'єктів;

– поширеність. Як відомо, розкриття злочину і покарання злочинця також в деякій мірі впливають на потенційних правопорушників. Тому розкривати часто зустрічаються типи злочинів при інших рівних важливіше, ніж рідкісні типи злочинів;

– кількість і кваліфікація персоналу. Залежно від того, скільки є співробітників і наскільки вони кваліфіковані, варто братися за ті чи інші комп'ютерні злочини. Занадто складні починати розслідувати марно;

– юрисдикція. Кращими є злочини, які не потребують задіяти іноземні правоохоронні органи. Найбільш швидкий результат виходить при розслідуванні злочинів, локалізованих в межах одного міста;

– політика.

11. Залежно від поточних політичних установок, можуть бути визнані більш пріоритетними деякі види комп'ютерних злочинів. Чи не тому, що вони більш суспільно небезпечні, але тому, що їх розкриття спричинить більший піар-ефект або більше схвалення начальства.

12. Спосіб вчинення наклепу, образ та екстремістські дії в глобальній комп’ютерній мережі Інтернет полягає, як правило, в розміщенні на загальнодоступному, як правило, популярному ресурсі в Інтернеті образливих, наклепницьких або екстремістських матеріалів.

13. Ресурси вчинення наклепу, образ та екстремістські дії в глобальній комп’ютерній мережі Інтернет можуть бути наступними: веб-форуми і дошки оголошень, веб-сторінки, повідомлення в телеконференціях (newsgroups), масова розсилка (спам) електронною поштою, СМС-повідомленнями та іншими системами обміну повідомленнями. Інші засоби вживаються нечасто.

14. DoS-атака або атака типу «відмова в обслуговуванні» є одним з видів незаконного втручання, а саме такого, який призводить до блокування інформації і порушення роботи ЕОМ і їх мережі. Інші види незаконного втручання (копіювання інформації, знищення інформації), а

також використання шкідливих програм можуть бути етапами здійснення DoS-атаки.

15. Організувати DoS-атаку на типовий веб-сайт не представляє з себе складного завдання, вона під силу IT-фахівця середньої кваліфікації, що має в своєму розпорядженні середнє ж обладнання і середньої ширини канал зв'язку.

16. Один тип DoS-атаки заснований на використанні вразливостей в програмному забезпеченні, що атакується ресурсу. Інший тип – так званий флуд – не використовує ніяких вразливостей і розрахований на просте вичерпання ресурсів жертви (смуга каналу, оперативна пам'ять, швидкодія процесора, місце на диску тощо).

17. Дефейс полягає в тому, що зловмисник тим або іншим способом змінює зовнішній вигляд публічного веб-сайту потерпілого, найчастіше його титульну сторінку. Технічно це можна здійснити, отримавши доступ на запис до директорії, де зберігаються дані вебсервера. Також часто дефейс виробляють, скориставшись вразливістю в самому веб-сервері або одному з його CGI-скриптів. Буває, що зловмисник змінює веб-сторінку, скориставшись штатної функцією, під аккаунтом одного із законних користувачів.

18. Однак, крім фіктивних інтернет-магазинів шахраї використовують і інші приводи для отримання платежів:

– псевдо-сайти благодійних організацій, релігійних організацій, політичних партій і рухів, які нібито збирають пожертви;

– спам-розсилки та сайти з проханням про матеріальну допомогу під зворушливу історію про бідну сирітку, жертві війни, заручника тощо;

– сайти фіктивних шлюбних агентств і окремі віртуальні нареченої;

– шахрайські онлайн «банки» і «інвестиційні фонди», які обіцяють величезні відсотки за вкладами;

– розсилки і сайти про нібито виявлені вразливості і чорних ходах в платіжних системах, що дозволяють множити свої гроші, наприклад,

переславши їх на особливий рахунок (в тому числі шахрайства II порядку, побудовані на тому, що жертва думає, ніби вона обманює обманщика);

– шахрайські сайти і розсилки, що пропонують віддалену роботу (на таку найчастіше клюють мережеві ескапісти) і вимагають під цим приводом будь-якої «вступний внесок».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Internet для користувача : [навч. посіб.] / В. М. Антоненко, Б. Д. Пацай, Л. О. Терейковська, І. А. Терейковський ; Держ. податк. адмін. України, Нац. ун-т держ. податк. служби України. — Ірпінь : НУ ДПС України, 2010. — 244 с. : іл., табл. — Бібліогр.: с. 227. — Предм. покажч.: с. 242–244.

2. Бишовець О.В. Психологічний вплив у кримінальному провадженні: теорія і практика : [монографія] / О.В. Бишовець. - К. : Істина, 2013. -152 с.

3. Біленчук П.Д. Балістика: криміналістичне вогнестрільне зброєзнавство : [підручник] / П.Д. Біленчук, А.В. Кофанов, В.Ф. Сулява ; [за редакцією проф. П.Д. Біленчука.] - К. : Міжнародна агенція "BeeZone", 2003. - 384 с.

4. Біленчук П.Д. Документування результатів слідчої дії: методи фіксації доказової інформації : [монографія] / П.Д. Біленчук, А.В. Кофанов, О.Л. Кобилянський, Л.Д. Скільська ; [за ред. П.Д. Біленчука]. - Київ : ННІПСК КНУВС, 2009. - 96 с.

5. Бірюков В.В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів : [монографія] / Бірюков Валерій Васильович / Луган. держ. ун-т внутр. справ ім. Е.О Дідоренка. - Луганськ : РВВ ЛДУВС їм. Е. О. Дідоренка, 2009. - 664 с.

6. Бутузов В.М. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток : Навчальний посібник / В.М. Бутузов, В.І. Василинчук, В.П. Шеломенцев. - К. : Типографія ТОВ "СТ-Стиль". - 2006. - 139 с.

7. Бутузов, Віталій Миколайович. Протидія комп’ютерній злочинності в Україні (системноструктурний аналіз) / В. М. Бутузов ; Рада нац. безпеки і оборони України, Міжвід. н.-д. центр з пробл. боротьби з

організованою злочинністю. — Київ. : КИТ, 2010. — 405 с. : табл., схеми. — Бібліогр. у підрядк. прим.

8. Волобуєв А.Ф. Розслідування і попередження розкрадань майна у сфері підприємництва : [навч. посібник] / А.Ф. Волобуєв ; [за ред. проф. О.М. Бандурки]. - Х. : "Рубікон", 2000. - 272 с.

9. Гора І.В. Криміналістика : [навч. посібник] / І.В. Гора, А.В. Іщенко, В.А. Колесник. - [4-те вид]. - К. : Вид. ПАЛИВОДА А.В., 2007 - 236 с.

10. Городецька, Оксана Степанівна. Комп’ютерні мережі та Інтернет : лаб. практикум / О. С. Городецька, Д. В. Михалевський ; М-во освіти і науки України, Вінниц. нац. техн. ун-т. — Вінниця : ВНТУ, 2017. — 75 с. : іл., табл. — Бібліогр.: с. 74-75.

11. Девтеров, Ілля Володимирович. Соціалізація людини у кіберпросторі / І. В. Девтеров ; Мво освіти і науки, молоді та спорту України, Нац. техн. ун-т України ”Київ. політехн. ін-т”. — Київ. : НТУУ ”КПІ”, 2012. — 357 с. — Бібліогр.: с. 335–357.

12. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.

13. Експертиза в судовій практиці / [за ред. В.Г. Гончаренка]. - К. : Юрінком Інтер, 2010. - 400 с.

14. Іщенко А.В. Методологічні проблеми криміналістичних наукових досліджень : [монографія] / А.В. Іщенко ; за ред. LH Красюка. - К. : Нац. акад. внутр. справ України, 2003. - 359 с.

15. Керівництво з розслідування злочинів : наук.-практ. посіб. / [кол. авт. : В.К). Шепітько, В.О Коновалова, В.А. Журавель та ін.] ; за ред. В.Ю. ГДепітька. - Х. : Одіссей, 2009. - 960 с.

16. Клименко НІ. Судова експертиза в розслідуванні комп'ютерних злочинів як форма використання спеціальних знань / НІ. Клименко, П.Д. Біленчук // Теорія та практика судової експертизи і криміналістики : 36. матер. міжнар. наук.-практ. конф. - Х. : Право, 2002. - Вип. 2. - С. 62-66.

17. Клименко НІ. Судова експертологія: курс лекцій : навч. посіб. для студ. юрид. спец. вищ. навч. закл. / НІ. Клименко. - К. : Видавничий Дім «Ін Юре», 2007. - 528 с.

18. Когутич 1.1. Криміналістичні знання, їх сутність і потреба розширення меж використання : монографія / 1.1. Когутич. - Львів : "Тріада плюс", 2008. - 420 с.

19. Кофанов А.В. Криміналістика: питання і відповіді : [навчальний посібник] / А.В. Кофанов, О.Л. Кобилянський, Я.В. Кузьмічов та ін. - К. : Центр учбової літератури, 2011. - 280 с.

20. Кравцова, Марина Олександрівна. Запобігання кіберзлочинності в Україні / М. О. Кравцова, О. М. Литвинов ; [за заг. ред. О. М. Литвинова] ; Кримін. асоц. України. — Харків : Панов, 2016. — 210 с. : іл., табл. — Бібліогр.: с. 191–210.

21. Криміналістика (криміналістична техніка) : [курс лекцій] / П.Д. Біленчук, А.П. Гель, М.В. Салтевський, Г.С. Семаков. - К. : МАУП, 2001. - 216 с.

22. Криміналістика : [навч.-метод. посібник] / В.В. Тіщенко, Л.І. Аркуша, В.М. Плахотіна. - [4-те вид., випр.]. - Одеса : Фенікс, 2013. – 338 с.

23. Криміналістика : [підруч. для студ. вищ. навч. закл.]. / [ред. В.Ю. Шепітько]. - К : Ін Юре, 2010. - 496 с.

24. Криміналістика : [підручник для студ. юрид. спец. ВЗО] / [ред. : В.Ю. Шепітько] // Нац. юрид. академія ім. Я. Мудрого. - Київ : Ін-Юре, 2004. - 725 с.

25. Криміналістика : [підручник] / В.Д. Берназ та ін. ; [за заг. ред. д-ра юрид. наук, проф. А.Ф. Волобуєва]. - Х. : ХНУВС, 2011. - 665 с.

26. Криміналістика : [підручник] / За ред. П.Д. Біленчука. - [2-ге вид., випр. і доп.]. - К. : Атіка, 2001. - 544 с.

27. Криміналістика : [підручник]. / В.М. Глібко, А.Л. Дудніков, В.А. Журавель, В.О. Коновалова, Г.А. Матусовський, З.І. Митрохіна, В.Ю. Шепітько ; [під ред. В.Ю. Шепітька]. - К. : Ін Юре, 2001. - 682 с.

28. Криміналістика : підручник / [Шепітько В.Ю., Коновалова В.О, Журавель В.А. та ін.] ; за ред. проф. В.Ю. Шепітька. - 4-е вид., перероб. і доп. - Х. : Право, 2008. - 464 с.

29. Криміналістика в тестах : [навч. посібник] / І.І. Когутич, (D.M. Колужна, І.В. Жолнович та ін. ; [за заг. ред. І.І. Когутича]. - К. : Але-рта, 2013. - 534 с.

30. Криміналістика. Академічний курс : підручник / Т.В. Варфоломеєва, В.Г. Гончаренко, В.І. Бояров та ін. - К. : Юрінком Інтер, 2011. - 504 с.

31. Криміналістика: Криміналістична тактика і методика розслідування злочинів : [підручник для студ. юрид. вузів і фак]. / В.О. Коновалова, Г.А. Матусовський, В.Ю. Шепітько, В.М. Глібко, А.Л. Дудніков. - Х. : Право, 1998. - 375 с.

32. Методика розслідування окремих видів злочинів: навч. посібник / О. І. Гарасимів, О. М. Дуфенюк, О. В. Захарова та ін.; за заг. ред. Є. В. Пряхіна. 2-ге вид., перероб. та допов. Львів: ЛьвДУВС, 2019. 312 с.

33. Міхайліна, Тетяна Вікторівна. Кримінальна відповідальність за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут / Т. В. Міхайліна ; М-во освіти і науки України, Донец. нац. ун-т. — Донецьк : ДонНУ, 2012. — 188 с.

34. Моделювання та аналіз безпеки розподілених інформаційних систем : навч. посіб. / [Литвинов В. В. та ін.] ; М-во освіти і науки України, Черніг. нац. технол. ун-т. — Чернігів : Черніг. нац. технол. ун-т, 2016. — 253 с.

35. Музика, Анатолій Ананійович. Законодавство України про кримінальну відповідальність за ”комп’ютерні” злочини: науково-

практичний коментар і шляхи вдосконалення / А. А. Музика, Д. С. Азаров. — Київ. : Паливода А. В., 2005. — 118, [1] с. — Бібліогр.: с. 108– 119 та у підрядк. прим.

36. Паламарчук, Л. П. Розслідування злочинів у сфері використання комп'ютерних технологій / Л. П. Паламарчук ; Київ. нац. ун-т ім. Т. Шевченка. — Київ : ЕксОб, 2007. — 143 с. — Бібліогр.: с. 124-143 та у підрядк. прим.

37. Правове регулювання відносин у мережі Інтернет / [А. П. Гетьман та ін.] ; за ред. С. В. Глібка, К. В. Єфремової ; НАПрН України, НДІ правового забезпечення інновац. розвитку. — Харків : Право, 2016. — 345, [1] с.

38. Система електронних платежів : навч. посіб. / [Бутузов В. М. та ін.] ; М-во освіти і науки, молоді та спорту України. — Київ. : Три К, 2013. — 292 с. — Бібліогр.: с. 279–290. — Предм. покажч.: с. 291–292.

39. Федотов, Олександр Анатолійович. Викриття злочинів у сфері комп'ютерних технологій як різновид боротьби з тероризмом / О. А. Федотов ; Нац. акад. внутр. справ. — Львів : Вид-во Львів. політехніки, 2014. — 219 с.

40. Щербаковський, Михайло Григорович. Розслідування комп'ютерних злочинів : навч. посіб. / М. Г. Щербаковський, Д. В. Пашнєв ; М-во внутр. справ України. — Харків. : Харк. нац. ун-т внутр. справ, 2010. — 111 с.