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

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ПОРУШЕННЯ ПРАВИЛ ЕКСПЛУАТАЦІЇ ЕОМ, АВТОМАТИЗОВАНИХ СИСТЕМ, КОМП'ЮТЕРНИХ МЕРЕЖ ЧИ МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ АБО ПОРЯДКУ ЧИ ПРАВИЛ ЗАХИСТУ ІНФОРМАЦІЇ, ЯКА В НИХ ОБРОБЛЮЄТЬСЯ

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

Виконала: студент 2 курсу 10-281 МЗ групи
Спеціальності 262 Правоохоронна діяльність
Освітньо-професійної програми
«Правоохоронна діяльність»
Гасанов Джавід Хаганійович

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

Херсон – 2021

ЗМІСТ

ВСТУП

Актуальність теми. У XIX ст. персональні комп’ютери, локальні комп’ютерні мережі та глобальна комп’ютерна мережа Інтернет отримують дедалі більше розповсюдження. Без них вже неможливе ефективне функціонування підприємств, установ та організацій всіх форм власності і, навіть, повсякденне життя окремих людей. Нажаль, цим активно користуються зловмисники, які з мотивів особистого збагачення, хуліганських мотивів, мотивів расової та релігійної ненависті усе частіше використовують персональні комп’ютери, локальні комп’ютерні мережі та глобальну комп’ютерну мережу Інтернет як об’єкти злочинних посягань та знаряддя вчинення злочинів.

Питання, пов’язані з розслідуванням комп’ютерних злочинів, раніше були предметом досліджень таких вчених, як Ю.М. Батурін, Т. В. Варфоломеєва, В. Д. Гавловський, О. І. Гарасимів, О. М. Дуфенюк, В. А. Журавель, О. В. Захарова, А. В. Іщенко, М. І. Камлик, В. О. Коновалова, В.В. Крилов, М.О. Ларкін, В. В. Пясковський, Б. В. Романюк, В. П. Сабадаш, М.В. Салтевський, А. В. Самодін, В. Ю. Шепітько, О.І. Усов, Ю. М. Чорноус. Зазначені вчені зробили істотний вклад в наукові дослідження, однак низка питань досі залишаються малодослідженою. Мова йде про питання, пов’язані з особливостями розслідування порушення правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них. Отже, удається за необхідне провести дослідження зазначених питань.

Мета і задачі дослідження. Метою дослідження полягає в дослідженні проблемних питань, пов’язаних із особливостями розслідування порушення правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та

комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них.

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

– дослідити нормативно-правове закріплення порушення правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них;

– проаналізувати типові слідчі ситуації та типові слідчі версії при розслідуванні порушення правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них;

– дослідити особливості призначення та проведення експертизи при розслідуванні порушень правил мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них;

– дослідити тактичні особливості проведення негласних слідчих (розшукових) дій при розслідуванні порушень правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них;

– дослідити тактичні особливості проведення допиту при розслідуванні порушень правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них

Об’єкт дослідження включає в себе суспільні відносини, пов’язані із дослідженням проблемних питань, пов’язаних із особливостями розслідування порушення правил користування мережами електрозв'язку, електронних обчислювальних машин, систем

та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них.

До **предмету цього дослідження** включено правові норми, результати наукових досліджень, які дають можливість дослідити проблемні питання, пов’язані з особливостями розслідування порушення правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них.

При обранні **методів дослідження** автор керувався метою та завданнями роботи, об’єктом та предметом наукового дослідження.

При проведенні дослідження використовувались загально наукові методи: аналізу, версії, аналогії, дедукції, індукції, синтезу, описовий, формально-юридичний, експериментальний, порівняльний, порівняльно-правовий, статистичний, системно-структурний.

Наукова новизна одержаних результатів відрізняю цю роботу, як таку, якою комплексно досліджено проблемні питання, пов’язані з особливостями розслідування порушення правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них.

Практичне значення роботи полягає у виявленні основних проблемних питань щодо особливостей розслідування порушення правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них. У роботі надані пропозиції, висновки, рекомендації, які можуть згодом можуть бути застосовані в подальших наукових дослідженнях та проведення навчальних занять з курсу «Кримінальний процес», «Криміналістика».

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 завданнями дослідження, а також метою наукового дослідження і включає вступ, двох розділів, які поділяються на п’ять підрозділів, висновки, список використаних джерел.

РОЗДІЛ 1
ЗАГАЛЬНІ ВИЗНАЧЕННЯ ЩОДО ПОРУШЕННЯ ПРАВИЛ КОРИСТУВАННЯ МЕРЕЖАМИ ЕЛЕКТРОЗВ'ЯЗКУ, ЕЛЕКТРОННИХ ОБЧИСЛЮВАЛЬНИХ МАШИН, СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ АБО ПОРЯДКУ ЧИ ПРАВИЛ ЗАХИСТУ ІНФОРМАЦІЇ, ЩО ОБРОБЛЮЄТЬСЯ У НИХ

1.1. Нормативно-правове закріплення порушення правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них

Слушним удається розгляд проблемних питань, пов’язаних із нормативно-правовим закріпленням порушення правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них.

«Об'єктом злочину є встановлений порядок експлуатації АЕОМ, їх систем чи комп'ютерних мереж» [30].

Проблеми нормативного закріплення зазначеного складу злочину, і, таким чином, подальшого його розслідування виникає вже на стадії законодавчого визначення основних термінів.

М. В. Рудик у своєму дослідженні «Засоби попередження настання суспільно небезпечних наслідків від порушення правил експлуатації АЕОМ» справедливо зазначає, що «законодавець не дає чіткого визначення таких правил, через що виникає питання, а що взагалі варто розуміти під правилами експлуатації автоматизованих електронно-обчислювальних систем? Перш за все, це суто технічні вимоги щодо догляду за комп'ютером, одночасно це і організаційно-правові норми, що мають за мету підпорядкувати та поставити під

охорону важливі суспільні відносини, пов’язані з безпечним використанням комп’ютерної інформації в автоматизованих електронно-обчислювальних системах. Отож, під правилами експлуатації автоматизованих електронно-обчислювальних систем слід розуміти комплекс технічно-організаційних заходів правового напрямку, головною метою якого було б підтримання автоматизованих електронно-обчислювальних систем в належному технічному стані, з одного боку, та протидія викраденню, перекрученню чи знищенню комп’ютерної інформації, засобів її захисту, або незаконному копіюванню комп’ютерної інформації, з іншого боку» [36].

«З об'єктивної сторони злочин даного виду характеризується недотриманням правил експлуатації мереж електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж. Вказане порушення вчиняється шляхом здійснення дій, або при бездіяльності. В останньому випадку обов’язковою умовою настання кримінальної відповідальності є спричиненні у результаті вчинення цього злочину суспільно небезпечних наслідків. Під правилами експлуатації мереж електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж вчені розуміють правила та регламенти, що визначають порядок роботи із вказаними приладами, а також системами та/або мережами, у які вони об’єднані, проведення за допомогою них, забезпечення захисту таких приладів та машин, їх систем та мереж або інформації, яка в них знаходиться, тощо. Захист інформації (у т.ч. комп'ютерної), що е власністю держави або захист якої гарантується державою, здійснюється з дотриманням правил, що встановлюються спеціально уповноваженим державним органом. На даний час таким органом є Департамент спеціальних телекомунікаційних систем та захисту інформації СБ. Порушення правил експлуатації АЕОМ, їх систем чи комп'ютерних мереж вважається злочинним лише у разі, коли його наслідком було: викрадення; перекручення чи знищення

комп'ютерної інформації, засобів її захисту; незаконне копіювання комп'ютерної інформації; істотне порушення роботи АЕОМ, їх систем чи комп'ютерних мереж. Зазначені негативні результати виникають або через недотримання встановлених правих експлуатації, або через злочинні дії кіберзлочинців, вчинення яких, у свою чергу, було полегшано або взагалі стало можливим через зазначені вище порушення правил експлуатації» [30].

Наприклад, «ОСОБА_2 у лютому 2014 року обіймаючи посаду адміністратора безпеки, для доступу до свого автоматизованого робочого місця (далі АРМ), яке є елементом КСЗІ ЗВІД ДП «УСС» та використовувалось ним для управління та моніторингу, створив пароль адміністратора безпеки Ncsathokm283», чим порушив вимоги п. 9 «Експертного висновку щодо оцінки КСЗІ ЗВІД ДП «УСС», а саме «паролі адміністратора безпеки та системного адміністратора на доступ до елементів КСЗІ мають довжину не менш ніж дванадцять символів, не містять поширених слів, використовують спеціальні символи». Надалі, у 2015 році ОСОБА_2, встановив на своєму АРМ адміністратора безпеки, операційну систему Windows 7 Professional, чим порушив вимоги п. 6.5.1.1. «Плану захисту інформації КСЗІ ЗВІД», а саме «Заборонене використання на АРМ, що використовуються для управління та моніторингу (АРМ адміністраторів та чергової зміни), серверах та активному мережевому обладнанні програмного забезпечення, що не відповідає наведеному в проектній документації». У відповідності до таблиці 3.1. «Опису програмного забезпечення КСЗІ ЗВІД» - для забезпечення функціонування .АРМ обслуговуючого персоналу КСЗІ ЗВІД має використовуватись операційна система Windows XP Professional SP2. Впродовж 2014-2015 років ОСОБА_2, для особистих потреб, встановив на своєму АРМ адміністратора безпеки наступні програмні засоби: «Skype», «NeroBurn», «ImageBurn» та ін., чим порушив вимоги п.6.5.1.1. «Плану захисту інформації КСЗІ ЗВІД», а

саме «Заборонене використання на АРМ, що використовуються для управління та моніторингу (АРМ адміністраторів та чергової зміни), серверах та активному мережевому обладнанні програмного забезпечення, що не відповідає наведеному в проектній документації». У таблиці 3.1. «Опису програмного забезпечення КСЗІ ЗВІД» вищевказані програмні засоби відсутні. 03.03.2014 між ДП «УСС» та Державною міграційною службою України (далі ДМСУ) укладено договір на закупівлю послуг щодо обробки даних (послуги з розміщення поштового серверу та веб-сайту (хостингу) із забезпеченням захищеного Інтернет-доступу до ресурсів веб-сайту та електронної пошти) № 15/11.18/14/КЛ. 12.03.2015 між ДП «УСС» та ДМСУ укладено договір на закупівлю послуг щодо обробку даних, послуг з розміщення поштового серверу та веб-сайту (хостингу) із забезпеченням захищеного Інтернет-доступу до ресурсів веб-сайту та електронної пошти) № 11.43/15/ін/11, у зв'язку із закінченням терміну дії попереднього. Відповідно до вказаного договору № 11.43/15/ін/11, ДП «УСС» надавало ДМСУ 200 Гб дискового простору на своєму сервері для функціонування поштового серверу та веб-сайту ДМСУ, а також забезпечувало захищений доступ до поштового серверу та веб-сайту ДМСУ, відповідно до вимог законодавства в галузі захисту інформації, через захищений вузол Інтернет-доступу ДП «УСС». Відповідальною особою за технічні питання з боку ДП «УСС», був призначений адміністратор безпеки КСЗІ ЗВІД ОСОБА_2. 16.10.2014 на веб-сервері сайту ДМСУ, невстановленими особами було створено нелегітимний обліковий запис користувача «ІНФОРМАЦІЯ_2». Надалі, у період 2015 року невстановленими особами, із використанням шкідливого програмного забезпечення, яке функціонувало на АРМ адміністратора безпеки ОСОБА_2, було скомпрометовано та отримано пароль адміністратора безпеки останнього. За допомогою отриманого паролю адміністратора безпеки, невстановлені особи надали нелегітимному обліковому запису

користувача «ІНФОРМАЦІЯ_2» Root-права для можливості входу до серверу ДМСУ і здійснення несанкціонованих дій з інформацією» [7].

Розглянемо інший випадок вчинення злочину вказаного виду.

«Наказом (розпорядженням) директора ТОВ «Кредмаш Сервіс» №89 від 18 червня 2013 року ОСОБА_4 призначена на посаду головного бухгалтера підприємства… Основні обов'язки, які мають виконувати головний бухгалтер або особа, на яку покладено ведення бухгалтерського обліку підприємства, визначені … чинним законодавством. Згідно посадової інструкції головного бухгалтера, затвердженої директором ТОВ «Кредмаш Сервіс» та з якою ОСОБА_4 ознайомлена у серпні 2013 року, більш точної дати досудовим розслідуванням не установлено, головний бухгалтер: керує працівниками бухгалтерського обліку підприємства та розподіляє між ними посадові завдання, обов'язки та ін. Таким чином, головний бухгалтер ТОВ «Кредмаш Сервіс» ОСОБА_4 здійснює організаційно-розпорядчі та адміністративно- господарські функції, відповідно до чинного законодавства є службовою особою. Відповідно до Додаткової угоди №1 до договору банківського рахунку №13-10-23-000682 від 23.10.2013 та заяви про підключення до системи «Клієнт-банк» в ПАТ «Діамантбанк» від 02.12.2013, ОСОБА_4 визначено особою, що має право на вирішення питань, пов'язаних з роботою системи «Клієнт-банк».Зокрема, за наявності на розрахунковому документі Клієнта «Візи №6», відповідальний виконавець Фронт-офісу Дирекції, Відділення/УДО - в обов'язковому порядку здійснює обробку платежу лише після отримання підтвердження Клієнта попередньо здійснивши його ідентифікацію». 06.02.2017, невстановленими особами, направлені до ПАТ «Діамантбанк» підроблені електронні платіжні доручення №8914 та №8915 на перерахування грошових коштів ТОВ «Кредмаш Сервіс». Близько 10 год, ОСОБА_4, відповідно до первинного листа непрацездатності А ДЕ №239267 від 06.02.2017 виданого Комунальним

закладом «Центр первинної медико-санітарної допомоги №4» перебуваючи на лікарняному, попередньо не перевіривши та не переконавшись у достовірності платіжних доручень №8914 та №8915, здійснила їх підтвердження представнику ПАТ «Діамантбанк». У зв'язку з цим, з розрахункових рахунків ТОВ «Кредмаш Сервіс», згідно платіжного доручення №8914 перераховано ТОВ «Хепінес» грошові кошти в розмірі 2 560 750,37 гривень та згідно платіжного доручення №8915 ФОП «ОСОБА_11» - в розмірі 396 840,15 гривень. У подальшому, на підставі ухвал Октябрського районного суду м. Полтави від 04.08.2017 року скасовано арешти з рахунку НОМЕР_1, відкритого на ФОП «ОСОБА_11» в ПАТ «Альфа-Банк» в межах суми 42 340,56 грн. та рахунку №26005645628700, відкритого на ТОВ «Хепінес» в АТ «УкрСиббанк»» в межах суми 1 229 810 грн. шляхом списання вказаних коштів на розрахунковий рахунок №26008060723670 в ПАТ КБ «ПриватБанк», який належить ТОВ «Кредмаш Сервіс». Внаслідок неналежного виконання до своїх службових обов'язків головним бухгалтером ОСОБА_4, з рахунків ТОВ «Кредмаш Сервіс» невстановленими особами, здійснено несанкціоноване перерахування грошових коштів загальною сумою 1 685 439,96 грн., чим підприємству заподіяно тяжкі наслідки у вигляді збитків на зазначену вище суму» [6].

«Суб'єкт зазначеного злочину спеціальний. Це особа, яка відповідає за експлуатацію АЕОМ, їх систем чи комп'ютерних мереж. Такою особою є користувач зазначених машин, систем чи мереж, а так само будь-яка інша особа, яка відповідно до своїх трудових, службових обов'язків або на основі відповідної угоди з власником (адміністратором) цих машин, систем та мереж виконує роботу, пов'язану з підтриманням їх у робочому стані, оновленням інформації, вдосконаленням АЕОМ, системи чи мережі, їх захистом чи іншу подібну роботу і зобов'язана при її виконанні дотримуватись встановлених правил експлуатації (і, зокрема, захисту) АЕОМ, систем та мереж» [30].

1.2. Типові слідчі ситуації та типові слідчі версії при розслідуванні порушення правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що обробляється у них

Слушним, на думку автора, удається розгляд проблемних питань, пов’язаних з типовими слідчими ситуаціями та типових слідчих версій при розслідуванні порушення правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що обробляється у них.

Адже вибір «гласної» та негласної слідчої (розшукової) дії, а також тактичних особливостей її проведення слід, на нашу думку, здійснювати з урахуванням слідчої ситуації, що склалася під час розслідування.

О. І. Гарасимів, О. М. Дуфенюк, О. В. Захарова у своїй роботі «Методика розслідування окремих видів злочинів» «наводять наступні типові слідчі ситуації початкового етапу розслідування: встановлено час несанкціонованого доступу до комп’ютерної інформації; відсутні відомості про спосіб доступу й особу (осіб), яка вчинила злочинні діяння; встановлені час і місце несанкціонованого доступу до комп’ютерної інформації; відомі особи, які володіють необхідними професійними знаннями, проте заперечують свою причетність до злочину; встановлено час несанкціонованого доступу до комп’ютерної інформації; відома особа (особи), яка зацікавлена в цій інформації, але відсутні відомості про спосіб доступу й особу (осіб), яка вчинила злочинні діяння; встановлено час несанкціонованого доступу до комп’ютерної інформації; є сліди, що вказують на конкретного

підозрюваного, але він заперечує свою причетність до вчиненого злочину; визначено місце злочинного заволодіння комп'ютерною інформацією, для здійснення якого використовувався механічний вплив; проте відсутні відомості про особу (осіб), яка вчинила дане діяння» [27].

О. І. Мотлях «виділяє три типові слідчі ситуації при розслідуванні кіберзлочинів:

– власник або користувач комп'ютерної мережі (бази даних) власними силами виявив факт незаконного проникнення й інших протиправних дій, знайшов винну особу і заявив про це у правоохоронні органи;

– власник або користувач комп'ютерної мережі (бази даних) інформаційної системи виявив факт незаконного проникнення й інших протиправних дій, але не зміг установити винної особи і заявив про це в правоохоронні органи;

– дані про порушення цілісності (конфіденційності) інформації в інформаційній системі і винну особу стали загальновідомими чи безпосередньо виявлені органом дізнання (наприклад, у ході проведення оперативно-розшукових заходів стосовно іншої справи)» [28].

«При розслідуванні кіберзлочинів можна виділити наступну систематизацію слідчих ситуацій:

1. Ситуації, що характеризуються наявністю персоналізованих відомостей про користувача як імовірного злочинця (розгорнуті анкетні дані особи).

2. Ситуації, що характеризуються наявністю неперсоналізованих відомостей про користувача як імовірного злочинця.

3. Ситуації, що характеризуються відсутністю будь-яких відомостей про особу злочинця. У межах кожної з груп таких слідчих ситуацій схарактеризовано три різновиди:

– ситуація, коли кримінальне провадження розпочато на підставі отримання заяви/повідомлення особи про кримінальне правопорушення;

– ситуація, коли кримінальне провадження розпочато внаслідок перевірки оперативної інформації;

– ситуація, коли кримінальне провадження розпочато в межах реалізації матеріалів ОРС. Розгляд ситуацій у комплексі з основними тактичними завданнями та комплексом слідчих (розшукових) дій та інших заходів пізнання визначає специфіку розслідування класифікаційних груп/підгруп злочинів, вчинених у кіберпросторі» [].

Також вид та порядок проведення негласної слідчої (розшукової) дії слід обирати виходячи із версій, висунутих під час розслідування.

О. І. Гарасимів, О. М. Дуфенюк, О. В. Захарова справедливо зазначають, що «типовими слідчими версіями під час розслідування кіберзлочинів є:

– «комп'ютерний» злочин учинений з метою отримання матеріальної вигоди.

– «комп'ютерний» злочин учинено з метою порушення авторських прав.

– «комп'ютерний» злочин учинено з метою порушення алгоритму обробки інформації, знищення або пошкодження комп'ютерних програм і баз даних, а також їх носіїв» [27].

Розгляд проблемних питань, пов'язаних із загальними визначеннями щодо порушення правил експлуатації мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них, дає можливість зробити наступні висновки:

1. Проблеми нормативного закріплення зазначеного складу злочину, і, таким чином, подальшого його розслідування виникає вже на стадії законодавчого визначення основних термінів.

2. Правила експлуатації зазначених пристроїв закріплені численними нормативними актами, а також відомчими інструкціями.

РОЗДІЛ 2
ОСОБЛИВОСТІ ПРОВЕДЕННЯ СЛІДЧИХ ДІЙ ПРИ РОЗСЛІДУВАННІ ПОРУШЕННЯ ПРАВИЛ МЕРЕЖАМИ ЕЛЕКТРОЗВ'ЯЗКУ, ЕЛЕКТРОННИХ ОБЧИСЛЮВАЛЬНИХ МАШИН, СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ АБО ПОРЯДКУ ЧИ ПРАВИЛ ЗАХИСТУ ІНФОРМАЦІЇ, ЩО ОБРОБЛЮЄТЬСЯ У НИХ

2.1. Особливості призначення та проведення експертизи при розслідуванні порушень правил мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них

Слушним удається розгляд проблемних питань, пов’язаних з особливостями призначення та проведення експертизи при розслідуванні порушень правил мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них.

О. І. Мотлях «до діагностичних завдань комп’ютерно-технічної експертизи відносить наступні завдання:

– визначення виду (типу, марки), властивостей апаратних засобів, а також їх технічних та функціональних характеристик;

– стан апаратних засобів, наявність поломок, дефектів;

– характеристика носіїв даних апаратних засобів;

– відтворення умов, обстановки, фактичних даних використання апаратних засобів на місці події.

– встановлення складу і кількісних характеристик програмно-комп’ютерний засобів;

– характеристика фактичного стану програмного забезпечення, окремих програм та наявність можливих у них відхилень;

– встановлення причинного зв'язку між діями користувача комп'ютерної системи відносно програмного забезпечення і наслідками, що наступили.

– характеристика та зміст інформації, що знаходиться на електронних комп'ютерних носіях;

– виявлення ознак втручання та внесення змін у інформаційні дані;

– встановлення механізму і обставин події виходячи з інформації, що знаходиться на комп'ютерних носіях та його копіях.

– загальна характеристика комп'ютерної мережі та її складових;

– використання типового комп'ютерно-мережевого оснащення та виявлення у них ознак відхилень від встановлених стандартів;

– причини внесення змін у комп'ютерно-мережеве забезпечення та імовірні наслідки їх застосування;

– встановлення зв'язку між зміною у комп'ютерно-мережевому оснащенні і суб'єктами, які співпрацюють з даним комп'ютерним забезпеченням» [28].

Слід також погодитись із вченими, які наголошують, що «Судова програмно-комп'ютерна експертиза визначає загальні характеристики операційної системи, її функціональні властивості, визначає фактичний стан програмного об'єкта, склад відповідних файлів, їх параметри тощо. Судова інформаційно-комп'ютерна експертиза встановлює властивості вид інформації у комп'ютерній системі, наявність відхилень від типових об'єктів (шкідливі включення, порушення цілісності тощо), встановлює первісний стан інформації на фізичних носіях та ін. Судова комп'ютерно-мережева експертиза визначає властивості й характеристики апаратного засобу і програмного забезпечення, встановлює місце, конфігурацію мережі та її компоненти, відповідність

виявлених характеристик типовим для конкретного класу засобів мережної технології тощо» [12].

Інші вчені слушно зазначають, що «об’єктами комп’ютерно-технічної експертизи виступають:

– зібрані комп’ютери, їх системні блоки;

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

– магнітні носії інформації (жорсткі диски і флопі-диски, оптичні диски);

– роздруківка програмних і текстових файлів;

– словники пошукових ознак систем (тезауруси), класифікатори та інша технічна документація, наприклад, технічні завдання і звіти; – електронні записні книжки, інші електронні носії текстової або цифрової інформації, технічна документація до них» [26].

Але, не дивлячись на наявні у літературі та нормативних актах переліки типових питань, які ставляться перед експертом під час призначення судової комп’ютерно-технічної експертизи, слушним удається у кожному конкретному випадку призначення такої експертизи користуватися допомогою спеціаліста, адже в жодному науковому дослідженні або нормативному акті неможливо передбачити нюанси всіх слідчих ситуацій, що можуть скластися при розслідуванні кіберзлочинів.

Перелічимо перелік завдань, які вирішуються комп’ютерно-технічними експертизами.

1. Пошук доказової інформації.

Пошук на комп'ютерному носії документів, зображень, повідомлень та іншої інформації, що стосується справи, в тому числі в неявному (віддаленому, прихованому, зашифрованому) вигляді.

Не слід, на нашу думку, конкретизувати вид та зміст відшукуваної інформації . Експерт цілком може самостійно вирішити, чи стосується той чи інший текст, зображення або програма до справи. В ході пошуку інформації експерту доводиться переглядати очима тисячі текстів та зображень. Зрозуміло, що неможливо роздрукувати і прикласти до висновку їх все – з тим, щоб потім слідчий вирішив, що з знайденого відноситься до справи. Експерт в будь-якому випадку змушений проводити первинну селекцію і приймати рішення, що саме з знайденого долучати. Змушений в силу обсягів інформації. Типовий обсяг архіву електронної пошти середнього користувача – мегабайти.

Для більш активного користувача обсяг поштових повідомлень може містити сотні мегабайт. Це не поміститься ні в один висновок (протокол). Тому експерта слід ознайомити з кримінальною справою або хоча б коротко викласти його фабулу в постанові про призначення експертизи. І запросити у нього пошук «будь-якої інформації, що відноситься до даної справи».

2. Відшукання цифрових «слідів» злочину.

Коли комп'ютер використовується як засіб доступу до інформації, що знаходиться в іншому місці, і коли доступ до інформації здійснюється на цьому комп'ютері – в обох випадках залишаються «цифрові» сліди, сліди у вигляді комп'ютерної інформації. Комп’ютерно-технічна експертиза може визначити, коли, за яких умов і яким чином здійснювався доступ. Хто його здійснював, комп’ютерно-технічна експертиза визначити не може. Лише в деяких випадках експерту вдається виявити деякі відомості про користувача досліджуваного комп'ютера.

Дії, які залишають сліди на комп'ютері або на носії інформації, включають: доступ до інформації, її перегляд, введення, зміна, видалення, будь-яку іншу обробку або зберігання, а також дистанційне управління цими процесами.

3. Аналіз програмного забезпечення.

Аналіз програм для ЕОМ на предмет їх приналежності до шкідливих, до інструментів для здійснення неправомірного доступу до комп'ютерної інформації, до спеціальних технічних засобів, призначених для негласного отримання інформації. А також аналіз функціональності програм, принципу дії, ймовірного їх джерела, походження, автора. Іноді необхідно більш глибоке дослідження програм. Тобто дослідження не просто їх властивостей і функціональності, а походження, особливостей взаємодії з іншими програмами, процесу створення, зіставлення версій. Таке глибоке дослідження має на увазі дизасемблювання програми, запуск під відладником (покрокове виконання), дослідження структури даних. Це предмет окремої експертизи, іноді її називають програмно-технічної. Не часто можна знайти експерта, що поєднує спеціальні знання з ІТ і по програмування. Тому рекомендується проводити дві окремі експертизи – перша вивчає вміст комп'ютерних носіїв, а друга особливості виявлених програм.

Однак, таке глибоке дослідження програм необхідно далеко не завжди. Наприклад, шкідливість програми – це сукупність її функцій. Шкідливість може встановити експерт-фахівець з інформаційних технологій. А ось для зіставлення об'єктного коду програми з фрагментом вихідного коду необхідна участь експерта-програміста.

4. Експертний аналіз часу вчинення кіберзлочину та його окремих етапів.

Завдяки наявності у комп'ютера внутрішнього енергонезалежного годинника та простановці в різних місцях тимчасових міток стає можливим визначити, коли і в якій послідовності користувач персонального комп’ютера обробляв різні дії. Навіть якщо внутрішній годинник комп'ютера був переведений вперед або назад (в тому числі неодноразово), все одно є можливість відновити правильний час і

правильну послідовність подій. Переведення годинника комп'ютера сам по собі залишає сліди. А якщо ще була і мережева взаємодія, тобто можливість зіставити моменти подій, зафіксовані комп'ютером, з подіями по інших джерелах і з'ясувати зрушення внутрішнього годинника. Вирішення цього завдання можливе навіть у тому випадку, якщо системний блок, що містить внутрішній годинник, чи не знаходиться в розпорядженні експертизи. Тільки по носію інформації (наприклад, жорсткий диск) можна отримати деякі відомості про послідовність подій. Чим більше інформацій на носії, тим повніше буде відновлена картина.

Експертним шляхом можливо виконати навіть так екзотичне завдання, як перевірка алібі підозрюваного, який стверджує, що в певний час працював за комп'ютером. В цьому випадку, хоча мова не йде про вчинення комп'ютерного злочину, для перевірки алібі потрібно призначити комп’ютерно-технічну експертизу.

5. Отримання інформації про користувача персонального комп’ютера, як про можливого суб’єкта вчинення кіберзлочину.

Оцінка кваліфікації та деяких інших особливостей особистості користувача досліджуваного комп'ютера. При досить інтенсивному використанні комп'ютера людина неминуче залишає в ньому «відбиток» власної особистості. Документи, фотографії, музика, листування, налаштування, оформлення, закладки, часовий режим роботи, підбір програм – все це індивідуалізує інформаційний вміст комп'ютера.

Все це відображає інтелект користувача, його емоції, нахили, здібності. Немає впевненості, що питання повністю лежить в сфері комп’ютерно-технічної експертизи. Для більш об’єктивного підходу така експертиза повинна бути комплексною, комп'ютерно-психологічною. У всякому разі, питання кваліфікації користувача персонального комп’ютера користувача в області ІТ точно в компетенції експерта, який проводить комп’ютерно-технічну експертизу. Звичайно,

для оцінки кваліфікації на досліджуваному носії повинні знаходитися відповідні об'єкти, результати інтелектуальної діяльності – написання користувачем програми, листування по нетривіальним технічних питань, складні програмні інструменти (наприклад, відладник). Слід зауважити, що некоректно ставити питання про встановлення особистості користувача комп'ютера. Будь-які висновки про особистість на основі знайдених на диску плодів інтелектуальної і творчої діяльності можуть носити лише вірогідний характер.

Таким чином, зазвичай перед експертом, який проводить комп’ютерно-технічну експертизу, ставляться наступні питання:

– чи містяться на об’єктах, наданих для дослідження, інформація, що має відношення до відповідного кримінального провадження;

– чи можуть об’єкти, надані на дослідження, використовуватись для отримання несанкціонованого доступу до локальної чи/та глобальної комп’ютерної мережі;

– чи вчинялись за допомогою об’єктів, наданих на дослідження, діяння, які мають відношення до обставин кримінального провадження, в рамках якого призначено експертизу, незаконні дії (якщо так, то які саме дії та коли);

– про ідентифікацію знайдених електронних документів, програм для ЕОМ, про ознаки користувачів комп'ютера;

– чи належать об’єкти, надані для дослідження, до шкідливого програмного забезпечення (якщо так, то до якого саме), якими є їхні властивості, чи могли об’єкти, надані для дослідження, бути використані для незаконних дій, за фактом яких розслідується кримінальне провадження, в рамках розслідування якого призначено відповідно комп’ютерно-технічну експертизу.

Не менш важливими є питання, які, на нашу думку, не можуть бути вирішені під час проведення комп’ютерно-технічних експертиз.

1. Чи є програмна продукція контрафактною.

Окремої роз'яснення потребують питання, пов'язані з контрафактними примірниками творів, представленого в цифровий (електронній) формі. Неприпустимо ставити перед експертом питання, чи є досліджуваний примірник програмного продукту контрафактним. Контрафактність – це питання правовідносин між правовласником і користувачем, але ніяк не питання стану екземпляра. Один і той же екземпляр може бути контрафактним і легальним (ліцензійним), в залежності від того, чи сплатив користувач вартість ліцензії, чи минув її термін, виконані чи ліцензійні умови та інших обставин.

Іншими словами, контрафактність – це юридичний, а не технічний факт. Встановлювати його експерт не може. Звичайно, експерт може знайти непрямі ознаки контрафактності, тобто такі особливості, які зазвичай зустрічаються на контрафактних примірниках і зазвичай не зустрічаються на ліцензійних. Але прямими доказами такі ознаки не будуть, оскільки контрафактний примірник легко перетворюється в ліцензійний шляхом укладення договору з правовласником або його представником (а це зводиться до сплати відповідної суми). І, навпаки, ліцензійна копія легко стає контрафактної при порушенні користувачем ліцензійних умов. В обох випадках сама копія при таких «перетвореннях» ні на біт не змінюється.

Перед експертом слід ставити питання про наявність ознак контрафактності – будь-яких або конкретних, які заздалегідь відомі слідчому.

Втім, серед юристів існує думка, що ніяких «ознак контрафактності» взагалі не буває. А ознаки виконання примірника твору не повинні піддаватися експертизі, оскільки їх наявність або відсутність не пов'язане з контрафактних примірників. Згідно до цієї точки зору, для доказу порушення авторських прав неодмінно слід встановити виробника примірника твору, довести відсутність у нього дозволу від правовласника і лише потім проводити експертизу

вилучених примірників з метою встановити, чи дійсно вони були виготовлені тим же способом, на тому ж обладнанні.

Наприклад, до правоохоронних органів потрапив компакт-диск з твором. Диск типу CD-R, записаний з використанням ПК, обкладинка видрукувана на ксероксі, голограма відсутня. Чи слід встановлювати і закріплювати за допомогою експертизи всі перераховані ознаки? Обговорювана позиція стверджує, що ні, не слід. Оскільки відсутня причинний зв'язок між кустарним виконанням і відсутністю згоди власника авторських прав. Слід доводити порушення авторських прав, що зводиться до доведенню відсутності дозволу, тобто договору, між виробником диска і правовласником, або між виробником і уповноваженим представником правовласника, або між виробником і суспільством по колективному управлінню авторськими правами. А метод виготовлення диска з фактом укладення такого договору ніяк не пов'язаний. Отже, ознаки виконання диска нічого не доводять.

2. Вартість програмного продукту.

Технічний фахівець не може визначити ні вартість програмного продукту, ні шкоди правовласнику. Вартість є предметом товарознавчої або економічної експертизи.

Ціноутворення на програмні продукти та цифрові фонограми – це окрема велика тема. Відбувається воно трохи інакше, ніж щодо матеріальних товарів. При цьому витрати виробника – далеко не найважливіший фактор. Якщо по відношенню до матеріального товару ціна на різних ринках для різних груп споживачів може відрізнятися і в 2, і в 3, і навіть в 5 разів (більше – навряд чи), то щодо «нематеріального» програмного забезпечення ціна може відрізнятися в нескінченне число разів навіть в межах однієї країни. Нерідкі випадки, коли правовласник передає право на використання програмного продукту (ліцензію) абсолютно безкоштовно для деяких споживачів, а з інших споживачів бере значні суми.

3. Правомірність доступу.

Експерт не може визначити правомірність доступу, що здійснювався з досліджуваного комп'ютера або на досліджуваний комп'ютер. Правомірність – це, як і контрафактність, факт юридичний, а не технічний.

Але експерт може визначити ряд інших фактів, які дозволять слідчому і суду кваліфікувати доступ як правомірний чи неправомірний. Це такі факти:

– до якої саме інформації здійснювався доступ (для подальшого вирішення питання, чи є вона охороняється законом комп'ютерною інформацією);

– чи робив власник інформації, до якої був здійснений доступ, якісь які заходи для її захисту і обмеження доступу (для вирішення питання про конфіденційність цієї інформації);

– присутній на електронному документі або носії гриф «комерційна таємниця» чи іншої гриф;

– чи є даний спосіб доступу загальноприйнятим способом для публічних мережевих ресурсів.

4. Оцінка змісту.

Експерт може знайти на досліджуваному комп'ютері (носії) тексти і повідомлення з певної тематики, проте він не має права оцінювати зміст цих текстів, їх авторство. Також експерт не може діяти в якості перекладача, якщо тексти на іншій мові. Можливо, виняток становить той випадок, коли в листуванні використовується жаргон або транслітерація. Хоча завдання в цьому випадку начебто лінгвістична, але відповідних фахівців серед звичайних лінгвістів немає. Це як раз той випадок, коли найкращий перекладач – не перекладач, а фахівець в предметній області. Для «перекладу» текстів з жаргону або з нестандартного трансліта можна призначити окрему комплексну експертизу – лінгвістично-комп'ютерну. А можна доручити експерту в

рамках комп’ютерно-технічної експертизи «перетворити знайдені тексти в доступну для сприйняття форму без зміни їх смислового змісту, а також роз'яснити використовувані в текстах спеціальні терміни і вирази».

Отже, на вирішення комп’ютерно-технічної експертизи не можна ставити такі питання:

– про ліцензійність/контрафактності примірників творів та комп’ютерних програм, записаних на досліджуваних носіях;

– чи було правомірним використання об’єктів, наданих на дослідження, у рамках подій, щодо яких розслідується кримінальне провадження, в рамках якого призначено комп’ютерно-технічну експертизу;

– питання щодо того, скільки коштують об’єкти надані на дослідження, у рамках подій, щодо яких розслідується кримінальне провадження, в рамках якого призначено комп’ютерно-технічну експертизу;

– питання, які полягають у перекладі на іншу мов об’єктів, наданих на дослідження, у рамках подій, щодо яких розслідується кримінальне провадження, в рамках якого призначено комп’ютерно-технічну експертизу.

2.2. Тактичні особливості проведення негласних слідчих (розшукових) дій при розслідуванні порушень правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них

Слушним удається розгляд тактичних особливостей проведення негласних слідчих (розшукових) дій при розслідуванні порушень правил користування мережами електрозв'язку, електронних обчислювальних

машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них.

Розглянемо тактичні особливості перехоплення інтернет-трафіка.

На основі аналізу вмісту, а також статистики мережевого трафіку можна визначити і довести вчинення користувачем багатьох дій в мережі, а також отримати інформацію про пристрій програм, інформаційних систем і мереж. Збір і аналіз мережевого трафіку певного комп'ютера може замінити вилучення і експертизу самого цього комп'ютера, оскільки дасть таку ж інформацію, а саме вміст електронної пошти, свідоцтва про перегляд веб-сайтів, про розміщення інформації в Мережі, про несанкціонований доступ до віддалених вузлів, про використання контрафактних програм. І в той же час перехопити трафік буває простіше, ніж знайти і вилучити в справному стані комп'ютер.

Інтернет-трафік, що відноситься до певного вузла, найпростіше перехоплювати поблизу цього вузла. У міру віддалення від нього зростає технічна складність перехоплення, але зате знижується організаційна складність. У міру віддалення від вузла падає надійність і, можливо, повнота перехоплення трафіку, але зате підвищується скритність. Місце перехоплення трафіку в значній мірі визначається наявністю можливостей конкретного правоохоронного органу. Для визначення місць і методів можливого перехоплення обов'язково залучення технічного спеціаліста. При цьому поширеною помилкою є залучення фахівця з апаратурі телефонного зв'язку. Такий фахівець, звичайно, доступніше, ніж IT-фахівець того ж рівня. «Телефоніст» краще розбирається в обладнанні, технологіях і протоколах зв'язку 1-го і 2-го рівня (фізичний і канальний). Але працювати на більш високих рівнях мережевих протоколів (3-7) він не здатний. А як раз на цих рівнях лежить більшість можливостей перехоплення трафіку.

Різних місць і методів для перехоплення мережевого трафіку занадто багато, щоб перерахувати їх тут. Виділимо лише організаційні варіанти:

– перехоплення за допомогою наявної у правоохоронців апаратури;
– перехоплення засобами оператора зв'язку;
– перехоплення власними засобами.

У переважній більшості випадків в перехоплювати трафік може міститися таємниця зв'язку або таємниця приватного життя. Тому необхідно отримувати судове рішення.

Перехоплення трафіку може бути реалізований на різних рівнях.

1. На фізичному рівні:

– за допомогою електричних і оптичних розгалужувачів;
– за допомогою безконтактних датчиків;
– за допомогою перехоплення сигналу (для Wi-Fi і інших бездротових протоколів).

2. На канальному рівні:

– за допомогою підключення до концентратора (хабу);
– за допомогою функції віддзеркалювання порту на комутаторі (свіч);
– а допомогою ARP-атак і проксінг трафіку;
– за допомогою установки сніфера на цільовому або транзитному вузлі.

3. На мережевому рівні:

– за допомогою зміни маршрутизації і проксінг трафіку;
– за допомогою вбудованих функцій брандмауера або системи виявлення атак (IDS).

4. На прикладному рівні:

– аналізом трафіку на проксі-сервері (для HTTP-трафіку);

– аналізом трафіку на сервері електронної пошти (для SMTP-трафіку).

Формулюючи технічне завдання для перехоплення трафіку, слід неодмінно прикинути обсяг інформації. При занадто широких умовах відповідний трафік може досягти астрономічних величин. Великий об'єм не вміститься на носії і тому не піддасться подальшого аналізу.

Наприклад, нас цікавлять дії користувача, що працює за домашнім комп'ютером, який підключений до Інтернету через місцеву домову мережу. У його трафіку ми хотіли б знайти докази неправомірного доступу до віддалених вузлів. Було б помилкою ставити завдання так: «перехоплення вихідного та вхідного трафіку комп'ютера з IP-адресою 10.0.0.6». Крім незаконного втручання підозрюваний також займається і іншою діяльністю. На його комп'ютері стоїть клієнт файлообмінних мереж із середнім сумарним трафіком 6 кбайт/с (500 Мбайт за добу, 50 вхідного і 450 вихідного). Крім того, в домовій мережі розташований файловий сервер з набором музики і фільмів.

Оскільки внутрішній трафік для користувачів безкоштовний і необмежений, підозрюваний викачує 1-2 фільми в день і трохи музики (1 Гбайт за добу). Внутрішньомережний службовий трафік складає за добу ще близько 2 Мбайт. Причому все перераховане - в автоматичному режимі, незалежно від присутності підозрюваного вдома. На цьому тлі добові 10 Мбайт веб-трафіку, 0,5 Мбайт електронної пошти і 0,2 Мбайт за протоколу ICQ просто губляться. А докази незаконного втручання містяться лише в останньому пункті. Перехоплення всього перерахованого трафіку (1,5 Гбайт на добу) за кілька днів зажадає диска дуже великої місткості, якого може і не виявитися в розпорядженні фахівця. І потім знайти в цій купі корисні 0,013% буде нелегко.

Якщо ж ми, щоб виключити внутрішньо-мережевий трафік, просимо фахівця перехоплювати інформацію за межами будинкової мережі, на виході з неї, то допустимо іншу помилку. Оскільки будинкова

мережа підключена до Інтернету не безпосередньо, а через пристрій, що здійснює трансляцію IP-адрес (NAT), то в цій точці ми не зможемо відрізнити трафік підозрюваного від трафіку всіх інших користувачів тієї ж домової мережі.

В описаній ситуації правильне формулювання завдання повинна виглядати приблизно так: «перехоплення вихідного та вхідного трафіку комп'ютера з MAC-адресою 00: 15: f2: 20: 96: 54, що відноситься до протоколів HTTP, telnet , SMTP, POP, IMAP, ICQ і має в якості IP-адреса призначення (destination) або походження (source) будь-які зовнішні IP-адреси, тобто, IP-адреса крім 10.0.0.0/8». Аналіз і інтерпретація перехопленого трафіку повинні проводитися експертом в ході ТКЕ. Замість експертизи можна оформити це як чергове ОРЗ, але тоді доказом в суді перехоплений трафік не буде.

До перехопленому трафіку для його аналізу необхідно докласти деяку інформацію про конфігурацію та стан комунікаційного устаткування , щоб в ході ТКЕ вміст трафіку можна було інтерпретувати впевнено, без припущень. Наприклад, для наведеного вище випадку для інтерпретації знадобиться конфігурація комутатора будинкової мережі, MAC-таблиця на відповідному його порту, а також конфігурація пристрою, що виробляє трансляцію адрес (NAT).

Статистика минулого трафіку збирається на багатьох пристроях.

Усі без винятку маршрутизатори, а також багато інші комунікаційні пристрої мають вбудовані функції для збору різноманітної статистики.

Статистика – це, звичайно, не перехоплення трафіку, вона не дає доступу до його вмісту. Але і з статистики можна чимало почерпнути для розслідування і для доведення комп'ютерних злочинів.

У найпростіших випадках на кожному інтерфейсі підраховується лише загальна кількість отриманих і відправлених байтів і пакетів. Налаштування за замовчуванням передбачають більш детальну

статистику. Повний архівування всього трафіку ведеться лише в рідкісних випадках і не для всіх протоколів

Часто статистика ведеться за форматом «netflow». Він передбачає запис відомостей про кожного «потоці» (flow), тобто серії пакетів, об'єднаних сукупністю IP-адрес, портів і номером протоколу.

За такою статистикою можна встановити:

– факт звернення певного вузла (комп'ютера, ідентифікованого IP-адресою) до іншого вузла;
– час поводження з точністю до інтервалу дискретизації (від 5 хвилин до 1 години);
– кількість переданого й отриманого трафіка;
– протокол;
– номера портів по обидва боки (для TCP і UDP).

Розглянемо особливості здійснення вибіркового перехоплення комп’ютерної інформації.

Перехоплення по сигнатурам використовується для захисту інформації в такому технічному засобі, як система виявлення атак (IDS). Вона шукає в переданих пакетах заздалегідь визначені послідовності байтів, відповідні спробам несанкціонованого доступу, активності шкідливих програм, іншим недозволеним або підозрілим діям. Аналогічно можна побудувати і аналіз трафіку підозрюваного – визначити характерні послідовності (сигнатури), відповідні підозрілим діям. І ловити тільки сесії, в яких зустрічаються ці сигнатури. Наприклад, підозрюваний користується послугами провайдера комутованого доступу та, отже, з'єднується з Інтернетом з використанням динамічного IP-адреси. Поряд з ним IP-адреси з тієї ж мережі використовують ще кілька сотень користувачів. Потрібно проконтролювати листування підозрюваного по електронній пошті. Для цього достатньо записувати все SMTP-сесії, які виходять з мережі, де розташований комп'ютер підозрюваного, в яких зустрічається відповідна

послідовність символів щоб виділити листи, спрямовані від підозрюваного будь-яким адресатам через будь-які проміжні вузли.

Для такого виборчого перехоплення можна використовувати майже будь-яку IDS. Багато з них підтримують досить складні сигнатури за багатьма умовами.

Розглянемо тактичні особливості дослідження логів веб-сервера.

Лог – це журнал автоматичної реєстрації подій, які фіксуються в рамках будь-якої програми. Зазвичай кожній події відповідає одна запис в балці. Зазвичай запис вноситься відразу ж після події (його початку або закінчення). Записи ці складаються в призначений файл самою програмою або пересилаються нею іншої, спеціалізованій програмі, призначеної для ведення і зберігання логів.

Отже, в логах можуть реєструватися абсолютно будь-які події – від приходу одиничного ethernet-фрейма до результатів голосування. Форма запису про подію також цілком залишається на розсуд автора програми. Формат лога може бути машинно-орієнтованим, а може бути пристосований для читання людиною.

Іноді логи орієнтовані на цілі безпеки та розслідування інцидентів. У таких випадках намагаються по можливості ізолювати логи від системи, події в якій вони фіксують. якщо зловмисник подолає засоби захисту і отримає доступ до системи, він, можливо, не зможе одночасно отримати доступ до логів, щоб приховати свої сліди.

Майже кожна дія, вироблене людиною при взаємодії з інформаційною системою, може відображатися в балці прямо або побічно, іноді навіть в декількох балках одночасно. І логи ці можуть бути розкидані по різних місцях, про які неспеціаліст навіть не здогадається.

Щоб дізнатися про дії зловмисника, отримати будь-які дані про нього за допомогою логів, необхідно:

– дізнатися, які комп'ютери та їх програми залучені у взаємодію;

– встановити, які події логуються в кожної із залучених програм;

– отримати всі зазначені логи за відповідні проміжки часу;

– дослідити записи цих логів, зіставити їх один з одним.

Розглянемо таку дію, як перегляд одним користувачем однієї веб-сторінки. Перерахуємо залучені в цю дію системи, які в принципі можуть вести логи подій:

– браузер користувача;

– персональний міжмережевий екран на комп'ютері користувача;

– антивірусна програма на комп'ютері користувача;

– операційна система користувача;

– DNS-сервер (Резолвер), до якого звертався браузер користувача перед запитом веб-сторінки, а також DNS-сервера (власники зон), до якого рекрсивнояких рекурсивно звертався цей Резолвер;

– все маршрутизатори по шляху від комп'ютера користувача до веб-сервера і до DNS-серверів, а також білінгові системи, на які ці {{1 }} маршрутизатори пересилають свою статистику;

– засоби захисту (міжмережевий екран, система виявлення атак, антивірус), що стоять перед веб-сервером і залученими DNS-серверами;

– веб-сервер;

– CGI-скрипти, що запускаються веб-сервером;

– веб-сервери всіх лічильників і рекламних банерів, розташованих на

– переглядається користувачем веб-сторінці (як правило, вони підтримуються незалежними провайдерами);

– веб-сервер, на який користувач йде за гіперпосиланням з переглядається;

– проксі-сервер (якщо використовується);

– АТС користувача (при комутованому з'єднанні з Інтернетом по телефонній лінії) або інше обладнання останньої милі (xDSL, Wi-Fi, GPRS тощо);

– обладнання з боку користувача і з боку веб-сервера.

Разом може набратися два-три десятка місць, де відкладаються взаємно скорелювати записи, що відносяться до одного-єдиної дії користувача – перегляду веб-сторінки.

При більш складних видах взаємодії з'являється ще більше місць, в яких можуть залишитися сліди дій користувача. Визначити всі ці місця і вказати, до кого саме слід звертатися за відповідними балками, – це завдання для IT-фахівця. Навіть самий просунутий слідчий не в змозі його замінити. Тому залучення фахівця в таких випадках обов'язково.

Логи веб-сервера є далеко не єдиним джерелом інформації про дії користувача.

Набір даних, які можна знайти в логах веб-сервера різниться залежно від типу веб-сервера і його налаштувань. Найчастіше за все в логах присутні наступні дані:

– IP-адреса клієнта;

– час запиту, включаючи часовий пояс;

– поля HTTP-запиту клієнта:

– ідентифікатор (логін) користувача, якщо присутній аутентифікація, метод,

– URL запитуваної веб-сторінки і окремі його елементи (домен, шлях, параметри), версія протоколу,

– дійсну IP (при доступі через неанонімні проксі-сервер),

– ідентифікаційний рядок браузера клієнта (включаючи мову і, реферер (referrer), тобто адреса веб-сторінки, з якої був здійснений перехід на дану сторінку,

– тип контенту відповіді веб-сервера (MIME type),

– будь-які інші поля;
– код відповіді веб-сервера (status code);
– розмір відповіді веб-сервера (без урахування HTTP-заголовка);
– помилки, що сталися при доступі до веб -сторінки;
– помилки при запуску CGI-програм.

Не маючи доступу до самого веб-сервера, зловмисник може фальсифікувати тільки поля HTTP-запиту. Цей запит повністю формується на стороні клієнта, тому при бажанні зловмисник може підставити в нього будь-які поля з будь-якими значеннями.

Інформація в лозі IP-адреси є надійним джерелом доказів. При цьому слід пам'ятати, що це може виявитися IP проксі-сервера або сокс-сервера або іншого посередника.

Інші поля – це внутрішні дані веб-сервера (код відповіді, розмір сторінки і т. п.), яким також можна довіряти.

Для перевірки достовірності даних логів веб-сервера застосовується зіставлення записів між собою, а також з іншими балками.

Наприклад, співробітники служби інформаційної безпеки інтернет-казино, аналізуючи логи веб-сервера, зауважили, що браузер одного з гравців, згідно полях його HTTP-запитів, підтримує українську мову мову. При цьому IP-адреса значився за Кореєю. Вказівки ж на корейську мову не було. Співробітники перевірили, з яких ще адрес звертався користувач під цим обліковим записом. Виявилося, що з єдиного IP. Було перевірено, які ще користувачі зверталися з цієї ж IP-адреси. Виявилося, що більше ніхто цей корейський IP-адреси не використовував. Але співробітник служби безпеки не заспокоївся і перевірив, які ще були звернення від браузера з таким же набором налаштувань (мова, версія браузера, версія ОС, дозвіл екрана, прийняті типи даних). Виявилося, що з такого ж браузера було зареєстровано більше 10 аккаунтів. Всі ці користувачі приходили з IP-адрес різних

країн, причому країна відповідала імені користувача. Але ідентичний набір налаштувань браузера всіх цих користувачів (включаючи підтримку української мови) викликав великі підозри. Коли ж співробітник зіставив періоди активності всіх підозрілих користувачів, він побачив, що вони не перетинаються. Співробітники служби безпеки зрозуміли, що мають справу з кардером, який реєструє аккаунти по викраденим карткам, користуючись сокссерверамі в різних країнах. Подальша перевірка це підтвердила.

Вчені слушно зауважують, що «злочинці намагаються унеможливити виявлення їх справжніх електронних адрес. Для цього вони використовують різні технології забезпечення анонімності роботи в мережі, а також програми безпечної передачі інформації. Ця обставина ускладнює встановлення місцезнаходження контактної особи. Серед головних способів забезпечення анонімності можуть застосовуватись: – проксі-сервери (HTTP, SOCKS 5 тощо); – VPN-сервери; – TOR та 2IP. Останнім часом, особливо після блокування російських соцмереж, популярним стало використання VPN-серверів, за допомогою яких забезпечується конфіденційність інформації і приховування IP-адреси користувача. Тому при підготовці запитів до Інтернет-провайдерів потрібно правильно вказувати назви сайтів та адреси електронної пошти, уважно дослідивши і вичитавши їх перед цим» [5].

Розглянемо проблемні питання, пов’язані із доказуванням фактів розміщення в глобальній комп’ютерній мережі «Інтернет» незаконних публікацій:

– неможливо провести безпосередній огляд розміщеної інформації (твори), оскільки бачити можна лише зображення на екрані, яке виникло внаслідок складних і не контрольованих процесів передачі, і перетворення спочатку розміщеної інформації;

– переважна більшість веб-сторінок - динамічні, їх контент залежить від часу, місця розташування користувача, його браузера, ряду випадкових чинників;

– доступ до інформації в мережі проводиться за посередництвом безлічі технічних засобів, про більшість з яких не відомо нічого певного;

– в багатьох випадках доступ проводиться в інтерактивному режимі, то є для отримання інформації потрібно прояв ініціативи з боку користувача;

– існує багато способів ввести в оману користувача, що переглядає інформацію, – щодо самого факту розміщення інформації, її змісту, адреси, часу;

– розміщену інформацію в ряді випадків досить просто і швидко прибрати або вона знищується сама з плином часу;

– Інтернет розглядається багатьма як якась область особливої свободи чи екстериторіальних зона, тому там існує багато засобів і можливостей для анонімізації, приховування слідів, кругової поруки;

– існуючі процесуальні норми розраховані були виключно на офлайнові документи і докази, в них рідко враховані технічні особливості комп'ютерних мереж.

У найпростішому випадку розміщення на веб-сайті зводиться до приміщення файлу в відповідну директорію на сервері. У більш складних випадках для розміщення інформації можуть знадобитися також наступні дії:

– реєстрація або придбання доменного імені, настройка DNS серверів для нього;

– установка і запуск веб-сервера;

– придбання послуги провайдера по організації і підтримці вебсервера (хостинг або колокація);

– налаштування веб- сервера;

– створення або модифікація вихідного коду * веб-сторінки на мові HTML, PHP та ін.;

– створення або модифікація CGI-скриптів для підтримки роботи веб-сайту;

– створення або замовлення художнього оформлення (дизайну) веб-сайту;

– настройка аутентифікації і авторизації на веб-сайті;

– повідомлення будь-яким способом адреси (URL) розміщеного файлу або відповідної веб-сторінки зацікавленим особам, рекламування такої адреси;

– відстеження роботи веб-сайту, його статистики відвідувань, тра Фіка, кількості завантажень розміщеної інформації, відгуків відвідувачів тощо.;

– оновлення, актуалізація розміщеної інформації;

– видалення або блокування розміщеної інформації.

Кожне із зазначених дій залишає «цифрові» сліди. Чим більше таких дій здійснював зловмисник, тим легше його ідентифікувати і згодом довести його провину.

Як видно, сліди можуть бути досить численними. Втім, в цьому розділі мова йде не про пошук і викритті особи, яка розмістила інформацію, а про доведення наявності в Мережі самої цієї інформації.

У вітчизняній слідчій практиці застосовуються наступні способи фіксації вмісту веб-сайту з метою отримання доказової інформації:

– роздруківка веб-сторінок через браузер;

– роздруківка + рапорт співробітника поліції;

– огляд веб-сайту слідчим з понятими;

– такий самий огляд, але за участю фахівця;

– відповідь оператора зв'язку (провайдера) на запит про вміст сайту;

– експертиза;

– нотаріальне посвідчення (огляд сайту нотаріусом).

Кожен із способів не бездоганний. Хоча браузер і вся система WWW орієнтовані на непідготовлених осіб, все ж спеціальні знання потрібні для того, щоб переконатися у відсутності помилок і навмисних фальсифікацій. Тому без участі фахівця коректність результату не гарантована. Застосування ж експертизи начебто позбавляє від можливих помилок. Але викликає сумнів той факт, що об'єкт експертизи (веб-сторінка, веб-сервер) знаходиться не в розпорядженні експерта, а досить далеко від нього.

Розглянемо особливості перегляду доказової інформації, розміщеної на сайті.

Ланцюг перетворення інформації на шляху її від серверу до користувача виглядає наступним чином:

– інформація на диску сервера;
– веб-сервер;
– браузер;
– зображення на екрані.

При проходженні вказаного ланцюга інформація зазнає суттєвих змін, які є численними та мають багато варіантів. На шляху від диску сервера до користувача інформація зазнає змін через динамічні веб-сторінки.

На самому початку ери WWW, в першій половині 1990-х, веб-сторінка була еквівалентна файлу на диску веб-сервера. Тобто, наприклад, при запиті користувачем веб-сторінки «http://example.com/folder/page.html» сервер, розташований за адресою «example.com», брав з локального диска з директорії «folder» файл «page.html» і відправляв його вміст користувачеві, лише додавши в початок службовий заголовок. Такі HTML-сторінки називаються статичними.

Потім з'явилися динамічні веб-сторінки. За запитом користувача веб-сервер не просто бере певний файл, а виконує більш складну послідовність дій. З файлу або групи файлів або з бази даних веб-сервер вибирає не просто HTML-код, а програму.

Потім ця програма виконується, а результат її виконання відображається браузером користувача. До того ж, виконання програми може здійснюватися:

– веб-сервером або одним з його модулів;
– зовнішньої програмою на стороні веб-сервера;
– браузером користувача або одним з його модулів;
– зовнішньої програмою на стороні користувача.

Зрозуміло, що вид динамічної веб-сторінки буде залежати від багатьох факторів, в тому числі від конфігурації ПО на боці користувача. В даний час практично всі веб-сторінки в Інтернеті – динамічні.

Зміни доказової інформації через особливості браузера.

Слід брати до уваги, що передається від веб-сервера до браузеру код (HTML-код з різними включеннями) не сприймається людиною безпосередньо. Цей код - лише набір команд браузеру по генерації зображення, яке вже сприймається людиною, а отже, може викликати будь-які правові наслідки. Хоча HTML і інші використовувані на веб-сторінках мови стандартизовані, один і той же код може інтерпретуватися по-різному в різних умовах. Відмінності в інтерпретації (поданні) одного і того ж коду різними браузерами, як правило, невеликі. Деякі дрібниці і нюанси в стандартах не описані. Деякі браузери трохи відхиляються від стандартів або мають власні розширення до стандартизованого формату. Все це не може привести до принципових відмінностей у зовнішньому вигляді сторінки.

Але є моменти, які можуть привести до принципових, то є змістовним відмінностей. Це перш за все включені в HTML-код

програми на інших мовах або об'єкти, які відображаються іншими, зовнішніми додатками. Отримавши в складі веб-сторінки такий об'єкт, браузер намагається знайти і завантажити модуль або іншої програми для виконання такого коду і відображення результатів. Такі зовнішні (по відношенню до браузеру) модулі та програми значно менше стандартизовані і можуть показувати користувачеві істотно відрізняються зображення чи не показувати нічого, якщо відповідного модуля або зовнішнього застосування не знайшлося.

Тому, фіксуючи вид веб-сторінки, слід встановити, яким саме браузером формується це зображення і відзначити в протоколі версію браузера. Ще більш важливо встановити, чи тільки браузер формує зображення на екрані, чи беруть участь в цьому інші модулі або зовнішні програми, а якщо беруть участь, то які саме.

2.3. Тактичні особливості проведення допиту при розслідуванні порушень правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них

Слушним удається розгляд проблемних питань, пов’язаних з тактичними особливостями проведення допиту при розслідуванні порушень правил користування мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них.

Розглянемо тактичні особливості допиту потерпілого та свідка при розслідуванні зазначених злочинів.

Комп'ютерна інформація має властивість легко і швидко втрачатися. Затримка при зборі доказів може привести до їх неотримання. Тому потерпілих і свідків треба опитати на предмет таких

доказів якомога швидше, не чекаючи офіційного допиту, або якнайскоріше допитати.

У потерпілих і очевидців слід дізнатися наступне.

У випадку вчинення злочину, пов'язаного з електронною поштою:

– адреси електронної пошти – кореспондента і його власну адресу;

– чи зберіглося повідомлення електронної пошти (лист), де саме воно збережено;

– якщо повідомлення збережено, попросіть передати його так, щоб були доступні всі службові заголовки, як це зробити, залежить від використовуваної програми-клієнта;

– яка програма-клієнт використовувалася або який веб-інтерфейс.

У випаду, якщо вчинено злочин, пов'язаний з веб-сайтами:

– який адреса (URL) веб-сайту;

– послугами якого інтернет-провайдера користується потерпілий;

– в який час (бажано точніше) він відвідував веб-сайт;

– чи зберігся у нього копія або скріншот цього веб-сайту.

У випаду, якщо вчинено злочин, пов'язаний з телеконференцій (newsgroups):

– послугами якого інтернет -провайдер користується потерпілий;

– яке ім'я телеконференції;

– через який ньюс-сервер здійснювався доступ до телеконференцій;

– яке використовувалося ПО для доступу до телеконференцій, не здійснювався цей доступ через веб-гейт;

– який subject і інші дані повідомлення;

– чи зберіглося повідомлення телеконференції, де саме воно збережено;

– якщо повідомлення збережено, треба попросити передати його так, щоб були доступні всі службові заголовки (як це зробити, залежить від використовуваної програми-клієнта).

При допиті свідків «слідчому потрібно з'ясувати такі питання:

– за яких обставин зазначена особа бачила (виявила) факт неправомірного доступу до операційної системи чи окремого об'єкту інформації;

– день, час, місце та обставини, що сприяли вчиненню комп'ютерного злочину;

– чи цікавився хто-небудь комп'ютерною інформацією, програмним забезпеченням, комп'ютерною технікою даного підприємства, організації, установи, фірми чи компанії;

– чи не з'являлись у приміщенні, де розміщена комп'ютерна техніка, сторонні особи, а також чи не зафіксовані випадки роботи співробітників з інформацією, яка не належить до їх компетенції;

– чи не було будь-яких збоїв у роботі операційної системи (відключення електропостачання, непланова перевірка комп'ютерного устаткування, ремонтні роботи тощо), якщо були, то які саме і хто їх проводив» [28].

«Під час початкових допитів свідків і потерпілих потрібно з'ясувати: для чого призначено персональний комп'ютер, комп'ютерна мережа та система; щодо кола осіб, які мали доступ до приміщень, в яких знаходилась комп'ютерна техніка, складові елементи комп'ютерних мереж та систем, які були знаряддям вчинення злочину та/або предметом злочинного посягання по кримінальному провадженню, в рамках якого проводиться допит; чи не бачила особа, допит якої проводиться по кримінальному провадженню, сторонню особу/осіб; питання про забезпечення захисту інформації, зокрема, інформації, яка стала предметом злочинного посягання по кримінальному провадженню, в рамках якого проводиться допит;

питання про особу/осіб, які надали доступ до інформації, яка стала предметом злочинного посягання по кримінальному провадженню, в рамках якого проводиться допит (хто надав доступ і на якій підставі); питання щодо розміру майнової шкоди, яка завдана вчиненим кримінальним правопорушенням» [26].

«Допит свідків та інших процесуальних суб'єктів у злочинах з інформаційними технологіями має ті самі умовні стадії, що і при традиційних діях:

– з'ясовуються необхідні дані про особу, яка допитується (заповнюються анкетні дані частини протоколу слідчої дії);
– вільна розповідь особи, що підлягає допиту;
– стадія запитань-відповідей;
– фіксація ходу та результатів допиту» [28].

Розглянемо тактичні особливості допиту підозрюваного та обвинуваченого при розслідуванні порушень правил експлуатації мереж електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них.

«Під час першого допиту потрібно, спонукаючи особу до дійового каяття, з'ясувати: чи були внесені зміни в роботу персональних комп'ютері, комп'ютерних систем та мереж, які стали об'єктом злочинного посягання по кримінальному провадженню, в рамках якого проводиться допит, якщо так, то які саме; які шкідливі програмні засоби, на думку допитуваної особи, використовувались зловмисниками при незаконному втручанні в роботу персональних комп'ютері, комп'ютерних систем та мереж, які стали об'єктом злочинного посягання по кримінальному провадженню, в рамках якого проводиться допит; чи існують, на думку особи, допит якої проводиться, дієві засоби зменшення розміру шкоди, яка спричинена злочином, по кримінальному провадженню, в рамках якого проводиться допит; чи передавались

допитуваною особою та/або іншими особами відомості про роботу персональних комп’ютері, комп’ютерних систем та мереж, які стали об’єктом злочинного посягання по кримінальному провадженню, в рамках якого проводиться допит» [27].

Розгляд проблемних питань, пов’язаних із особливостями проведення слідчих дій при розслідуванні порушення правил мережами електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж або порядку чи правил захисту інформації, що оброблюється у них, дає можливість зробити наступні висновки:

1. Під час призначення судової комп’ютерно-технічної експертизи, слушним удається у кожному конкретному випадку призначення такої експертизи користуватися допомогою спеціаліста, адже в жодному науковому дослідженні або нормативному акті неможливо передбачити нюанси всіх слідчих ситуацій, що можуть скластися при розслідуванні кіберзлочинів.

2. При призначенні комп’ютерно-технічної експертизи не слід, на нашу думку, конкретизувати вид та зміст відшукуваної інформації.

3. При призначенні комп’ютерно-технічної експертизи експерт цілком може самостійно вирішити, чи стосується той чи інший текст, зображення або програма до справи. В ході пошуку інформації експерту доводиться переглядати очима тисячі текстів та зображень. Неможливо роздрукувати і прикласти до висновку їх все – з тим, щоб потім слідчий вирішив, що з знайденого відноситься до справи. Експерт в будь-якому випадку змушений проводити первинну селекцію і приймати рішення, що саме з знайденого долучати.

4. Коли комп'ютер використовується як засіб доступу до інформації, що знаходиться в іншому місці, і коли доступ до інформації здійснюється на цьому комп'ютері – в обох випадках залишаються «цифрові» сліди, сліди у вигляді комп'ютерної інформації.

5. Комп’ютерно-технічна експертиза може визначити, коли, за яких умов і яким чином здійснювався доступ. Хто його здійснював, комп’ютерно-технічна експертиза визначити не може. Лише в деяких випадках експерту вдається виявити деякі відомості про користувача досліджуваного комп'ютера.

6. При проведенні комп’ютерно-технічної експертизи глибоке дослідження програм необхідно далеко не завжди. Наприклад, шкідливість програми – це сукупність її функцій. Шкідливість може встановити експерт-фахівець з інформаційних технологій. А ось для зіставлення об'єктного коду програми з фрагментом вихідного коду необхідна участь експерта-програміста.

7. Завдяки наявності у комп'ютера внутрішнього енергонезалежного годинника та простановці в різних місцях тимчасових міток стає можливим визначити, коли і в якій послідовності користувач персонального комп’ютера обробляв різні дії.

8. Навіть якщо внутрішній годинник комп'ютера був переведений вперед або назад (в тому числі неодноразово), все одно є можливість відновити правильний час і правильну послідовність подій.

9. Переведення годинника комп'ютера сам по собі залишає сліди. А якщо ще була і мережева взаємодія, тобто можливість зіставити моменти подій, зафіксовані комп'ютером, з подіями по інших джерелах і з'ясувати зрушення внутрішнього годинника. Вирішення цього завдання можливе навіть у тому випадку, якщо системний блок, що містить внутрішній годинник, чи не знаходиться в розпорядженні експертизи.

10. Тільки по носію інформації (наприклад, жорсткий диск) можна отримати деякі відомості про послідовність подій. Чим більше інформацій на носії, тим повніше буде відновлена картина.

11. При досить інтенсивному використанні комп'ютера людина неминуче залишає в ньому «відбиток» власної особистості. Документи, фотографії, музика, листування, налаштування, оформлення, закладки,

часовий режим роботи, підбір програм – все це індивідуалізує інформаційний вміст комп'ютера.

12. Все це відображає інтелект користувача, його емоції, нахили, здібності. Немає впевненості, що питання повністю лежить в сфері комп’ютерно-технічної експертизи. Для більш об’єктивного підходу така експертиза повинна бути комплексною, комп'ютерно-психологічною.

13. У всякому разі, питання кваліфікації користувача персонального комп’ютера користувача в області ІТ точно в компетенції експерта, який проводить комп’ютерно-технічну експертизу.

ВИСНОВКИ

Розгляд проблемних питань, віднесених до теми дослідження, дає можливість зробити наступні висновки:

1. Проблеми нормативного закріплення зазначеного складу злочину, і, таким чином, подальшого його розслідування виникає вже на стадії законодавчого визначення основних термінів.

2. Правила експлуатації зазначених пристроїв закріплені численними нормативними актами, а також відомчими інструкціями.

3. Під час призначення судової комп’ютерно-технічної експертизи, слушним удається у кожному конкретному випадку призначення такої експертизи користуватися допомогою спеціаліста, адже в жодному науковому дослідженні або нормативному акті неможливо передбачити нюанси всіх слідчих ситуацій, що можуть скластися при розслідуванні кіберзлочинів.

4. При призначенні комп’ютерно-технічної експертизи не слід, на нашу думку, конкретизувати вид та зміст відшукуваної інформації.

5. При призначенні комп’ютерно-технічної експертизи експерт цілком може самостійно вирішити, чи стосується той чи інший текст, зображення або програма до справи. В ході пошуку інформації експерту доводиться переглядати очима тисячі текстів та зображень. Неможливо роздрукувати і прикласти до висновку їх все – з тим, щоб потім слідчий вирішив, що з знайденого відноситься до справи. Експерт в будь-якому випадку змушений проводити первинну селекцію і приймати рішення, що саме з знайденого долучати.

6. Коли комп'ютер використовується як засіб доступу до інформації, що знаходиться в іншому місці, і коли доступ до інформації здійснюється на цьому комп'ютері – в обох випадках залишаються «цифрові» сліди, сліди у вигляді комп'ютерної інформації.

7. Комп’ютерно-технічна експертиза може визначити, коли, за яких умов і яким чином здійснювався доступ. Хто його здійснював, комп’ютерно-технічна експертиза визначити не може. Лише в деяких випадках експерту вдається виявити деякі відомості про користувача досліджуваного комп'ютера.

8. При проведенні комп’ютерно-технічної експертизи глибоке дослідження програм необхідно далеко не завжди. Наприклад, шкідливість програми – це сукупність її функцій. Шкідливість може встановити експерт-фахівець з інформаційних технологій. А ось для зіставлення об'єктного коду програми з фрагментом вихідного коду необхідна участь експерта-програміста.

9. Завдяки наявності у комп'ютера внутрішнього енергонезалежного годинника та простановці в різних місцях тимчасових міток стає можливим визначити, коли і в якій послідовності користувач персонального комп’ютера обробляв різні дії.

10. Навіть якщо внутрішній годинник комп'ютера був переведений вперед або назад (в тому числі неодноразово), все одно є можливість відновити правильний час і правильну послідовність подій.

11. Переведення годинника комп'ютера сам по собі залишає сліди. А якщо ще була і мережева взаємодія, тобто можливість зіставити моменти подій, зафіксовані комп'ютером, з подіями по інших джерелах і з'ясувати зрушення внутрішнього годинника. Вирішення цього завдання можливе навіть у тому випадку, якщо системний блок, що містить внутрішній годинник, чи не знаходиться в розпорядженні експертизи.

12. Тільки по носію інформації (наприклад, жорсткий диск) можна отримати деякі відомості про послідовність подій. Чим більше інформацій на носії, тим повніше буде відновлена картина.

13. При досить інтенсивному використанні комп'ютера людина неминуче залишає в ньому «відбиток» власної особистості. Документи, фотографії, музика, листування, налаштування, оформлення, закладки,

часовий режим роботи, підбір програм – все це індивідуалізує інформаційний вміст комп'ютера.

14. Все це відображає інтелект користувача, його емоції, нахили, здібності. Немає впевненості, що питання повністю лежить в сфері комп’ютерно-технічної експертизи. Для більш об’єктивного підходу така експертиза повинна бути комплексною, комп'ютерно-психологічною.

15. У всякому разі, питання кваліфікації користувача персонального комп’ютера користувача в області ІТ точно в компетенції експерта, який проводить комп’ютерно-технічну експертизу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абрамова В.М. Криміналістика : [навч. посіб. для дистанційного навчання] / [В.М. Абрамова, А.О. Ляш]; за наук. ред. А.В. Іщенка. - К. : Університет "Україна", 2007. - 557 с.

2. Алексеев О.О. Розслідування окремих видів злочинів : навч. посіб. 2-ге вид. перероб. та доп. / О.О. Алексеев, В.К. Весельський, В.В. Пясковський - К. : "Центр учбової літератури", 2014. - 320 с.

3. Антонов, Валерій Миколайович. Інтернет : енцикл. вид. : [навч.-метод. посіб.] / Антонов В. М. ; [редкол.: Жалдак М. І. (голова) та ін.] ; АПН України, Ін-т інформ. технологій і засобів навчання. — Київ. : ТОВ Ред. «Комп'ютер», 2008. — 127 с. : іл., табл. — (Бібліотека вчителя інформатики; 2). — Бібліогр.: с. 127.

4. Бахін В.П. Шляхи формування професійної майстерності експерта / [Бахін В.П., Калініченко О.Л.] // Криміналістичний вісник. - К, 2005. - Вип. 2(4). - С. 66-71.

5. Використання електронних (цифрових) доказів у кримінальних провадженнях [Текст] : метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. — Вид. 2-ге, доп. — Київ : Вид-во Нац. акад. внутр. справ, 2020. — 104 с.

6. Вирок Автозаводський районний суд м. Кременчука Полтавської області по справі № 524/6552/17 URL: https: //reyestr.court.gov.ua/ Review/75827069).

7. Вирок Шевченківського районного суд м. Києва по справі № 761/11540/16-к URL: https://reyestr.court.gov.ua/Review/57555595 (дата звернення 1.10.2021).

8. Воротинський, Вадим Володимирович. Політичне маніпулювання в Інтернет-просторі України: політико-інституційний вимір : автореф. дис. … канд. політ. наук : 23.00.02 / Воротинський Вадим Володимирович ;

М-во освіти і науки України, Харків. нац. пед. ун-т ім. Г. С. Сковороди. — Харків, 2016. — 17 с. — Бібліогр.: с. 14-15.

9. Горбаньов, Ігор Миколайович. Особливості методики розслідування порушень авторського права щодо незаконного відтворення та розповсюдження комп'ютерних програм / Горбаньов І. М. ; Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. — Луганськ : Рєзніков В. С., 2012. — 199 с. : іл. — Бібліогр.: с. 165-196 та у підрядк. прим.

10. Гумінський, Руслан Вікторович. Методи і засоби виявлення інформаційних загроз віртуальних спільнот в інтернет середовищі соціальних мереж : автореф. дис. … канд. техн. наук : 21.05.01 / Гумінський Руслан Вікторович ; М-во освіти і науки України, Нац. авіац. ун-т. — Київ, 2016. — 20 с. : іл., табл. — Бібліогр.: с. 17–18.

11. Електронний банкінг : (організаційно-правове забезпечення) / [Новацький А. М. та ін. ; за заг. ред. А. М. Новацького] ; Нац. ун-т держ. податк. служби України, Наук.-дослід. Центр з пробл. оподаткування, Наук.-дослід. центр прав. інф-ки при Акад. прав. наук України. — Ірпінь : Нац. ун-т ДПС України, 2008. — 294 с. — Бібліогр.: с.207-218.

12. Іщенко А. В., Колесник В. А., Гора І. В. Криміналістика: Посіб. для підгот. до іспитів /А.В. Іщенко, В.А. Колесник, І.В. Гора. – 2-е вид., допов. та перер. – К.: Вид-во ПАЛИВОДА А.В., 2004. – 232 с.

13. Комп'ютерне моделювання інформаційно-аналітичних систем / О. Г. Додонов, О. В. Коваль, Л. С. Глоба, Ю. Д. Бойко ; НАН України, Ін-т проблем реєстрації інформації. — Київ : ІПРІ НАН України, 2017. — 238 с. : іл. — Бібліогр.: с. 225–238.

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

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

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

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

18. 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.

19. 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.

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

21. 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.

22. Криміналістична техніка : [навч. посібник] / В.В. Арешонков, І.М. Ганжа, О.В. Літвінова та інш ; [за ред. А.В. Кофанова]. - К. : "КИЙ", 2006. - 456 с.

23. Криміналістична техніка. Книга друга : [навч. посібник] / В.В. Арешонков, П.Д. Біленчук, О.Г. Волошин та інш. ; [за ред. А.В. Кофанова]. -К. : "КИЙ", 2009. - 416 с.

24. Лук’янчук, Руслан Валерійович. Державне управління у сфері забезпечення кібербезпеки України : автореф. дис. … канд. наук з держ. упр. : 25.00.01 / Лук’янчук РусланВалерійович ; Ін-т законодавства Верхов. Ради України. — Київ, 2017. — 19 с. — Бібліогр.: с. 14-16.

25. Методи аналізу та моделювання безпеки розподілених інформаційних систем / [В. В. Литвинов та ін.] ; за заг. ред. С. М.

Шкарлета ; М-во освіти і науки України, Черніг. нац. технол. ун-т. — Чернігів : Черніг. нац. технол. ун-т, 2017. — 204 с.

26. 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.

27. 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.

28. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. ... канд. юрид. наук : 12.00.09 / О. І. Мотлях ; Академія адвокатури України. – Київ, 2005. – 20 с.

29. 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.

30. Науково-практичний коментар Кримінального кодексу України від 5 квітня 2001р. / За ред. М.І.Мельника, М.І.Хавронюка. – К., 2001. – 1104 с.

31. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / Бутузов В. М. [та ін. ; за ред. Б. В. Романюка, Є. Д. Скулиша] ; Рада нац. безпеки і оборони України, Міжвідом. н.-д. центр з пробл. орг. злочинності, Служба безпеки України, Нац. акад. служби безпеки України. — Київ. : [б. в.], 2011. — 403, [1] с. : іл., [6] арк. кольор. іл. — Бібліогр.: с. 264-310.

32. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток: наук.-практ. посіб. / Бутузов В. М. [та ін.] ; [за ред. І. В. Бондаренка] ; Рада нац. безпеки і оборони України,

Міжвідом. наук.-дослід. центр з пробл. боротьби з орг. злочинністю. — Київ. : [б. в.], 2009. — 182 с.

33. Практикум з криміналістики : [навч. посібник] / В.Ю. Шепітько, В.О. Коновалова, В.А. Журавель та ін.; [за ред. В.Ю. Шепітька]. - К. : Ін Юре, 2013. - 128 с.

34. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [Користін О. Є. та ін.] ; за заг. ред. Коваленка В. В. ; Рада нац. безпеки і оборони України [та ін.]. — Київ : Скіф, 2012. — 722 с.

35. Розслідування злочинів у сфері господарської діяльності: окремі криміналістичні методики : [монографія] / Кол. авторів: В.Ю. Шепітко, В.О. Коновалова, В.А. Журавель та ін.; [за ред. В.Ю. Шепітька]. - Х. : Право, 2006. - 624 с.

36. Рудик, М. В. Засоби попередження настання суспільно небезпечних наслідків від порушення правил експлуатації АЕОМ / М. В. Рудик // Вісник Національного університету внутрішніх справ. - 2004. – Вип. 27. - С. 53-56

37. Салтевський М.В. Криміналістика (у сучасному викладі) : підручник / М.В. Салтевський. - К. : Кондор, 2008. - 588 с.

38. Самойленко О. А. Виявлення та розслідування злочинів в сфері ІТ-технологій [Текст] : навчальнометодичний посібник / О. А. Самойленко. Одеса : , 2020. 133 с.

39. Слідчий огляд: сутність, види, тактика проведення огляду місця події і тактика використання техніко-криміналістичних засобів та спеціальних знань : монографія / В.О. Комаха та інші ; [за заг. ред. В.О. Комахи] ; Одеська національна юридична академія. - Дніпропетровськ : ІМА-прес, 2004. - 396 с.

40. Снігур, Анатолій Васильович. Основи роботи в Internet : навч. посіб. / А. В. Снігур, І. Р. Арсенюк, І. С. Колесник ; М-во освіти і науки

України, Вінниц. нац. техн. ун-т. — Вінниця : ВНТУ, 2016. — 104 с. : іл., табл. — Бібліогр.: с. 104.

41. Тішенко В.В. Теоретичні і практичні основи методики розслідування злочинів : [монографія] / В.В. Тішенко // Одеська національна юридична академія. - О. : Фенікс, 2007. - 260 с.

42. 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.